угрозу только на ресурс, при этом на ресурсе располагаются следующие компоненты: операционная система, прикладное программное обеспечение, а также сама ценная информация, хранящаяся и обрабатываемая на ресурсе. Нарушение функционирования, целостности или конфиденциальности любого из этих элементов может привести к потере ценной информации — навигационной информации.

Для контроля программных угроз от локального нарушителя предлагается использовать метод орбитального мониторинга инцидентов по вине оператора системы ГЛОНАСС.

Суть предлагаемого метода орбитального мониторинга заключается в следующем: на борту каждого космического аппарата ГЛОНАСС устанавливается комплект навигационной аппаратуры потребителей (НАП). Она принимает сигналы от других спутников системы, в область диаграммы направленности которых попадает данный космический аппарат. Принимая штатный сигнал, на борту аппарата с помощью НАП можно измерить псевдодальность до источника излучения по временной задержке прохождения сигнала. Кроме того, в состав штатного сигнала входит информация о координатах излучившего его спутника (эфемериды). По принятым и известным собственным координатам космического аппарата можно рассчитать еще одно значение псевдодальности до источника сигналов. Определив разность между измеренным и рассчитанным значениями псевдодальности и сравнив ее со значением предельно допустимой погрешности, можно сделать вывод о достоверности излучаемой информации.

Для реализации данного метода необходима некоторая модификация передающего и антенного устройства бортовой аппаратуры всех спутников системы, а также установка на борту каждого космического аппарата многоканальной НАП, что возможно осуществить при дальнейшем развитии космических аппаратов «ГЛОНАСС». Необходимо отметить, что данная модификация БА навигационных спутников имеет также положительный «побочный эффект» — навигационное поле ГНСС «ГЛОНАСС» станет доступным низкоорбитальным космическим аппаратам, в том числе и пилотируемым, что будет неоспоримым конкурентным преимуществом перед американской GPS.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральная целевая программа. ГЛОНАСС/ГНСС-Форум. URL: http://aggf.ru/proekt/zakon/doc.php?zakID=2.
2. Федеральное космическое агентство. Информационно-аналитический центр. URL: http://www.federalspace.ru/main.php?id=3&nid=13077.

Е. С. Степанова, И. В. Кансафаров

ПРОГРАММНЫЙ МОДУЛЬ РЕАЛИЗАЦИИ АЛГОРИТМА ЧИСЛЕННОЙ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Повышение эффективности систем защиты информации (СЗИ) обусловливает необходимость разработки методического обеспечения, затрагивающего вопросы анализа рисков нарушения информационной безопасности.

На основе модели угроз в виде нечеткой когнитивной карты [1] разработаны метод и алгоритм оценивания риска нарушения ИБ, сущность которого сводится к следующему:

1. На основе политики безопасности, принятой в организации, с учетом категорирования информационных ресурсов, обрабатываемых в сегментах сети организации, строится матрица разграничения прав доступа;

2. На основе матрицы разграничения прав доступа на уровне строятся *матрицы угроз* несанкционированного доступа (НСД) и утечек;

3. Строится нечеткая когнитивная карта (НКК), *визуализирующая пути распространения угроз* НСД и утечки, с учетом матриц угроз и числа точек входа в систему. Причем веса влияния $w_{z,z+1}$ соответствуют значениям уязвимостей компонентов инфраструктуры – программного обеспечения, коммуникационного оборудования, протоколов связи и сервисов безопасности, представленных в НКК промежуточными концептами K_{z+1}^{j};

4. Задаются значения весов влияния в НКК, полученные на основе нормализации оценок уязвимостей, приведенных в [2].

5. Задаются значения вероятностей активизации источников угроз $\rho_{акт}$ и вероятностей наличия защищаемой информации в трафике $\rho_{ООИ}$;

6. Вычисляются вероятности реализации угрозы на *j*-м пути по формуле:

$$P_j = \rho_{акт} \cdot \rho_{ООИ} \cdot \prod_{z \in Z} w_{z,z+1};$$

7. Определяется максимальное значение из P_j, где $j \in [1, J]$, принимаемое в качестве оценки вероятности реализации угрозы $P^U(K_i \to K_y)$;

8. Вычисляются вероятности реализации угроз на информационные ресурсы с уровнями конфиденциальности «Н», «С», «В»;

9. Задаются численные значения *относительных стоимостей* информационных ресурсов в сегментах сети;

10. Вычисляются величины относительного риска нарушения информационной безопасности сегментов сети по формулам:

$$\overline{R_{CH}} = \sum_{n=1}^{N} \rho_{CH_n}{}^{U} \cdot \frac{Cm_{CH_n}}{Cm_{\Sigma}}, \; n \in [1, M],$$

$$\overline{R_{CC}} = \sum_{m=1}^{M} \rho_{CC_m}{}^{U} \cdot \frac{Cm_{CC_m}}{Cm_{\Sigma}}, \; m \in [1, M],$$

$$\overline{R_{CB}} = \sum_{l=1}^{L} \rho_{CB_l}{}^{U} \cdot \frac{Cm_{CB_l}}{Cm_{\Sigma}}, \; l \in [1, L],$$

где N, M, L – число сегментов, в которых хранится и обрабатывается информация категорий «Н», «С», «В» соответственно;

$\frac{Cm_{CH_n}}{Cm_{\Sigma}}, \frac{Cm_{CC_m}}{Cm_{\Sigma}}, \frac{Cm_{CB_l}}{Cm_{\Sigma}}$ – относительные стоимости информационных ресурсов, обрабатываемых в сегментах C_n^H, C_m^C и C_l^B соответственно.

11. Вычисляется относительный полный риск (в процентах) на объекте защиты по формуле:

$$\overline{R} = \overline{R_{C\text{Н}}} + \overline{R_{C\text{С}}} + \overline{R_{C\text{В}}}.$$

Программный модуль имеет интуитивно понятный интерфейс и представляет собой пошаговое выполнение вышеописанного алгоритма оценки риска нарушения ИБ.

В ходе работы с программным модулем пользователь формирует матрицу разграничения прав доступа с учетом политики безопасности, принятой в организации.

На основе матриц разграничения прав доступа программный модуль формирует матрицы угроз НСД и утечки с возможностью их последующей корректировки пользователем.

На основе матриц угроз программный модуль формирует пару: входной и выходной концепты нечеткой когнитивной карты. Пользователь последовательно указывает барьеры на пути распространения угроз между источником угрозы – входным концептом и информационным

ресурсом – выходным концептом. Данные о значениях вероятностей преодоления барьеров получены из базы данных [2].

В программном модуле предусмотрена функция сохранения проекта на любом этапе работы с возможностью последующего дополнения и изменения. Также предусмотрена функция формирования отчета, содержащего сведения об используемых сервисах безопасности, значениях относительного риска нарушения ИБ сегментов сети и относительного полного риска.

Программный модуль позволяет оценить риски нарушения информационной безопасности при проектировании системы защиты информации, сравнить в количественном отношении различные варианты наборов средств защиты для построения СЗИ.

Программный модуль разработан в среде Borland C++.

СПИСОК ЛИТЕРАТУРЫ:

1. *Степанова Е. С., Машкина И. В., Васильев В. И.* Разработка модели угроз на основе построения нечеткой когнитивной карты в проекции на топологию сети // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 2. Таганрог: Изд-во ТТИ ЮФУ, 2010. С. 232–239.
2. National Vulnerability Database (NVD) Search Common Platform Enumeration. URL: http://web.nvd.nist.gov/view/cpe/search.

М. С. Чистяков, А. П. Дураковский

ОСНОВЫ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ СРЕДСТВ ИЗГОТОВЛЕНИЯ И РАЗМНОЖЕНИЯ ДОКУМЕНТОВ

Следует отметить, что в настоящее время в сфере создания защищенных автоматизированных систем и оценки защищенности средств вычислительной техники остро обозначается проблема применения автоматизированных комплексов оценки защищенности. Проблема состоит в том, что такие комплексы могут быть полезны лишь при участии опытного оператора на каждом этапе проведения исследований. Алгоритмы автоматической выборки и верификации сигналов далеки от совершенства. Таким образом, многие специалисты в области специальных исследований (СИ) предпочитают автоматическому более трудоемкий, но и более точный процесс проведения измерений и расчетов в полуавтоматическом режиме. Проведение СИ вручную и явилось основной целью данной работы. Не любое средство изготовления и размножения документов (СИРД) подвержено утечке информации по каналам ПЭМИН. Проведем некоторую классификацию.

Существует большой выбор критериев классификации СИРД, однако нас интересует лишь один, имеющий значение для оценки защищенности СИРД от утечки информации по каналу ПЭМИН. За критерий классификации возьмем возможность преобразования информации, представленной в виде некоторых физических параметров (области на листе бумаги), в некоторый внутренний код устройства (двоичный код в общем случае). Удобно использовать классификацию по типу внутреннего представления информации. Тогда все СИРД можно будет разбить на две большие группы: информация преобразуется во внутренний код и информация не преобразуется во внутренний код.

Таким образом, первым шагом при проведении СИ некоторого СИРД необходимо определить принцип его работы и, как следствие, целесообразность специальных исследований.