1.2.2.

[1]А.Д. Ковалёв, [2]Д.В. Кондратов

[1]Саратовский государственный технический университет имени Ю.А. Гагарина,
Саратов, kovalev.ad13@gmail.com,
[2]Саратовский государственный технический университет имени Гагарина Ю.А.,
Саратов,
Институт проблем точной механики и управления
Российской академии наук (ИПТМУ РАН), Саратов,
Саратовский национальный исследовательский государственный университет
имени Н.Г. Чернышевского),
Саратов, kondratovdv@yandex.ru

ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ВОЗМОЖНОГО ВОЗНИКНОВЕНИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ПРЕДПРИЯТИЙ НА ОСНОВЕ СЕТИ ПЕТРИ

В статье поднимается актуальная проблема обеспечения безопасности защищаемых сведений после проведения работ по определению и защите от утечки по техническим каналам инструментально-расчетным методом. На основании анализа существующих научных работ по данной тематике вырабатывается одно из возможных решений данной проблемы на основе сетей Петри. Строится универсальная математическая модель, позволяющая определить возможность возникновения технических каналов утечки информации, тем самым сохранить защищаемые ресурсы.

Ключевые слова: *математическое моделирование, сети Петри, технический канал утечки информации, мультиграф, множество.*

Одной из главных задач сохранения защищаемой информации после проведения инструментально-расчетным методом работ по определению и защите от утечки по техническим каналам является выполнение требований отчетных документов по окончанию данного вида работ. Но, не редко, бывают случаи изменения каких-либо внешних факторов, не зависящих от рабочего персонала объектов информатизации, вследствие которых, могут быть нарушены условия эксплуатации. В данном случае, мы не будем рассматривать человеческий фактор, который чаще всего и является главной угрозой безопасности информации на объектах.

Проведя анализ научных работ [1-3] можно сказать, что большинство проводимых исследований направлены на построение системы защиты информации от утечки по техническим каналам до ввода в эксплуатацию объекта информатизации. Но нельзя исключать случаи, когда в существующей системе могут образоваться бреши. Именно поэтому мы и рассмотрим построение модели, способной определить защищенность системы после проведения работ по защите данных от утечки по техническим каналам.

Рассмотрим каналы утечки информации, присущие объектам информатизации, обрабатываемым информацию без ее звуковоспроизведения:

- побочное электромагнитное излучение элементов, содержащихся в технических средствах приема, обработки, хранения и передачи информации (ТСПИ);
- просачивание информационного сигнала в линии электропитания, заземления;
- наводки электромагнитных излучений элементов ТСПИ на посторонние проводники, находящиеся в зоне 1;
- перехват информации путем высокочастотного облучения ТСПИ;
- соответствие между распечатываемым символом и его акустическим образом;

- паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг к другу линий передачи данных;

- возникновение электромагнитного поля вокруг кабеля передачи данных при прохождении информационных сигналов;

- подключение к линиям связи;

- фото-, видео-, видовая съемки мониторов и других объектов отображения защищаемой информации ТСПИ. [4]

После проведения работ, специалистами сторонних компаний, имеющими лицензию на данный вид деятельности, все вышеуказанные каналы не могут быть использованы злоумышленником для кражи информации.

Рассмотрим случаи, при которых может быть нарушена система технической защиты информации. Например, одним из способов перехвата информации является его просачивание в цепи электропитания и (или) заземления. Рассмотрим случай, при котором электропитание защищаемого объекта информатизации будет перенесено с ближайшей точки подключения к трансформаторной подстанции, находящейся в пределах контролируемой зоны, на подстанцию за ее пределами, из-за выхода из строя и последующего ремонта линий. Данный канал был неактуален, а на время ремонта он становится брешью в защите охраняемого объекта.

Такие простые примеры можно найти для каждого канала утечки. Исходя из этого, возникает возможность возникновения утечки информации. Данная проблема стоит очень остро, и для ее вероятного решения, рассмотрим применение модели на основе сетей Петри.

Сети Петри представляет собой ориентированный мультиграф, состоящий из вершин двух типов – позиций и переходов, соединенных между собой дугами [5]. Получаемая, с помощью сетей Петри, модель служит для отображения и анализа причинно-следственных связей в системе [6].

Теория сетей Петри, во многих своих аспектах, теснейшим образом связана с теорией автоматов, и по существу является развитием последней. Это обстоятельство позволяет с единых методологических позиций рассматривать вопросы программного обеспечения, аппаратной поддержки и информационного обмена при проектировании вычислительных систем [7]. Не смотря на самостоятельность теории сетей Петри [8], она отражает часть общих тенденций современного анализа и моделирования, используемую специалистами во многих сферах. Основными можно выделить представление в графическом виде процессов и состояний систем, и применение информационных единиц как основы информационного языка и основы построения информационных конструкций [9] и информационных моделей [10].

Рассмотрим процесс возникновения технического канала утечки информации и построим математическую модель, которая поможет специалистам по информационной безопасности сохранить результат, т.е. оставить информацию конфиденциальной.

Представим на рис. 1 мультиграф, состоящий из совокупности множеств M = {P, U, S, I, O}, где

P = {P1, P2 … Pn}, (n - количество каналов утечки информации по техническим каналам);

U = {U1, U2…Ui}, (i – количество условий для появления технического канала утечки);

S = {S1, S2…S};

I –функция перехода;

O – выходная функция.

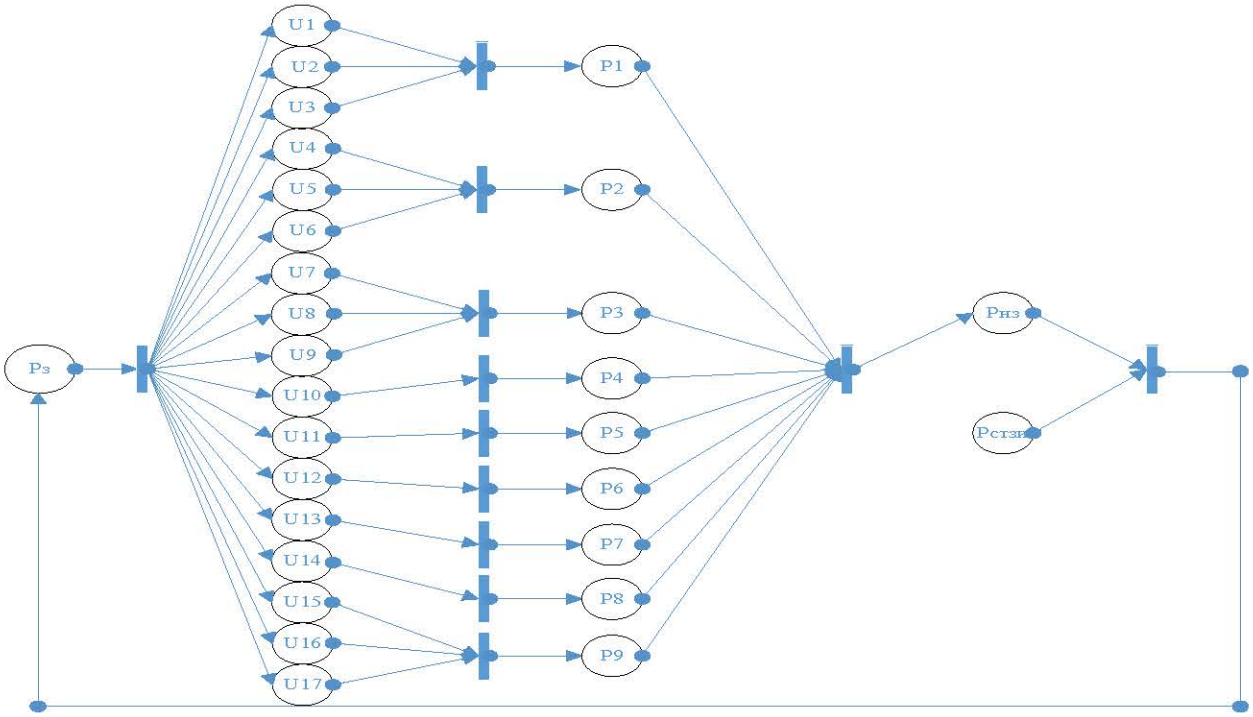

Рис. 1 – Модель возможного возникновения технических каналов утечки информации на объектах информатизации предприятия

Описание позиций, представленных на модели процесса возможного возникновения технических каналов утечки информации на объектах информатизации предприятий:

- Рз – состояние, в котором защищаемая информация не может быть доступна злоумышленнику.

Такое состояние актуально после проведения работ по инструментально-аналитическому контролю объекта информатизации и выдаче отчетных документов по результатам работ.

- Рнз – состояние, в котором защищаемая информация может быть доступна злоумышленнику.

- Рстзи – состояние, в котором по n-ому каналу утечки информации установлено средство защиты информации от утечки по техническим каналам и инструментально-аналитическим методом проведен контроль эффективности защиты, либо проведены работы по устранению организационными (техническими) методами канала утечки.

Перечень средств защиты информации от утечки по техническим каналам с действующими сертификатами соответствия можно найти на официальном сайте Федеральной службы по техническому и экспортному контролю [11] и Федеральной службы безопасности России [12].

Также стоит отметить, что в основном средства защиты информации от утечки по техническим каналам своим функционалом способны закрыть несколько каналов утечки одновременно, что стоит учитывать при их выборе.

- Р1 – позиция, в которой защищаемая информация может быть доступна посредством утечки по каналу побочных электромагнитных излучений элементов, содержащихся в ТСПИ.

- Р2 – позиция, в которой защищаемая информация может быть доступна посредством просачивания информационного сигнала в линии электропитания, заземления.

- Р3 – позиция, в которой защищаемая информация может быть доступна посредством наводок электромагнитных излучений элементов ТСПИ на посторонние проводники, находящиеся в зоне 1.

- Р4 – позиция, в которой защищаемая информация может быть доступна посредством перехвата информации путем высокочастотного облучения ТСПИ.

- Р5 – позиция, в которой защищаемая информация может быть доступна посредством поиска соответствия между распечатываемым символом и его акустическим образом.

- P6 – позиция, в которой защищаемая информация может быть доступна посредством паразитных емкостных, индуктивных и резистивных связей и наводок близко расположенных друг к другу линий передачи данных.

- P7 – позиция, в которой защищаемая информация может быть доступна посредством возникновения электромагнитного поля вокруг кабеля передачи данных при прохождении информационных сигналов.

- P8 – позиция, в которой защищаемая информация может быть доступна посредством подключения к линиям связи.

- P9 – позиция, в которой защищаемая информация может быть доступна посредством фото-, видео-, видовая съемки мониторов и других объектов отображения защищаемой информации ТСПИ.

- U1 – позиция, которая характеризует изменение контролируемой зоны в меньшую сторону.

- U2 – позиция, которая характеризует несанкционированное изменение состава ТСПИ.

- U3 – позиция, которая характеризует присутствие в зоне 2 технических средств, которые могут стать средством разведки.

- U4 – позиция, которая характеризует изменение положения питающих кабелей объектов информатизации.

- U5 – позиция, которая характеризует изменение положения токопроводящих конструкций.

- U6 – позиция, которая характеризует увеличение сопротивления заземлителя.

- U7 – позиция, которая характеризует изменение в меньшую сторону (перемещение ТСПИ) расстояния до токопроводящих линий, имеющих выход за пределы контролируемой зоны.

- U8 – позиция, которая характеризует проведение в зоне 1 транзитных линий связи или электропитания.

- U9 – позиция, которая характеризует уменьшение расстояния до вспомогательных технических средств.

- U10 – позиция, которая характеризует возможность нахождения облучающего устройства на расстояниях, с которых может вестись облучение и последующий прием высокочастотного сигнала, промодулированного защищаемой информацией.

- U11 – позиция, которая характеризует возможность размещения высокочувствительного микрофона с диктофоном в непосредственной близости с клавиатурой ТСПИ.

- U12 – позиция, которая характеризует возможность размещения в непосредственной близости от ТСПИ линий связи других объектов.

- U13 – позиция, которая характеризует возможность установки аппаратуры злоумышленника рядом с кабелем передачи информации.

- U14 – позиция, которая характеризует возможное подключение к линиям связи, не входящим в состав объекта информатизации.

- U15 – позиция, которая характеризует возможность проведения фото-, видео-, видовой съемки мониторов.

- U16 – позиция, которая характеризует возможность проведения фото-, видео-, видовой съемки мониторов или других средств отображения информации.

- U17 – позиция, которая характеризует возможность попадания видовой информации в поле зрения проходящих сотрудников, не имеющих определенного отношения к обрабатываемой информации.

Математическая модель, построенная на основе сетей Петри, для определения возможности возникновения технических каналов утечки информации на объектах информатизации предприятий является хорошим инструментом для выполнения задачи сохранения защищаемой информации. Разделение на множества условий позволяет специалистам по информационной безопасности в ходе изменения действующих методов и алгоритмов защиты совершенствовать данную модель и унифицировать ее под свои задачи.

Таким образом, предложена общая математическая модель для определения возможности возникновения технических каналов утечки информации на объектах информатизации предприятий. Представленная математическая модель позволяет выделить все основные канала утечки информации и, при необходимости, для конкретного предприятия оставить только актуальные канал. Также, обязательно стоит отметить, что данная модель характеризует возможность возникновения каналов утечки, потому как для хищения защищаемого ресурса нужно иметь ввиду наличие факта проведения разведки и оборудования, способного к данному виду разведки.

Список литературы

1. *Авсентьев О.С., Вальде А.Г.* Вербальная модель защиты информации от утечки по техническим каналам в процессе формирования системы защиты информации на объектах информатизации // Вестник Воронежского института МВД России. – 2022. – № 2. – С. 18-27.
2. *Белоглазов Е.Г.* Моделирование технических каналов утечки информации с целью улучшения их защищенности // Fractal simulation. – 2015. – № 1. – С. 5-11.
3. *Карпов А.В., Лепешкин О.М.* Моделирование технических каналов утечки информации на распределенных объектах управления // Международный журнал перспективных исследований. – 2018. – Т.8, № 2. – С. 69-83.
4. *Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.* Технические средства и методы защиты информации. Учебник для вузов / 7-е изд,. испр. – М.: Горячая линия – Телеком, 2023. - 444 с: ил.
5. *Питерсон Дж.* Теория сетей Петри и моделирование систем. – М.: Мир, 1984. – 264 с.
6. *Нестеровский О.И., Звягин Д.С., Жмыхова А.А.* Моделирование каналов утечки акустической информации при помощи сетей Петри // Вестник Воронежского института МВД России. – 2022. – № 1. – С. 40-46.
7. *Проститенко О.В.*, Моделирование дискретных систем на основе сетей Петри: учебное пособие / О.В. Проститенко, В.И. Халимон, А.Ю. Рогов. – СПб.: СПбГТИ (ТУ), 2017. – 69 с.
8. *Котов В.Е.* Сети Петри. – М.: Наука, 1984. –160 с.
9. *Tsvetkov V.Ya.* Information Constructions // European Journal of Technology and Design, 2014, Vol.(5), № 3 – p147-152.
10. *Breeden D., Viswanathan S.* Why do firms hedge? An asymmetric information model //Fuqua School of Business, Working Paper. – 1998.
11. Государственный реестр сертифицированных средств защиты информации [Электронный ресурс]. – Режим доступа: http://reestr.fstec.ru/reg3 (дата обращения 13.02.2024).
12. Выписка из перечня средств защиты информации, сертифицированных ФСБ России [Электронный ресурс]. – Режим доступа: http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_100124.doc (дата обращения 13.02.2024).