Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: **mathmod.esrae.ru/46-184**
Ссылка для цитирования этой статьи:
Ковалёв А.Д. Подбор параметров для построения математической модели оценки рисков возникновения технических каналов утечки информации на объектах информатизации предприятий // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2024. №2

УДК 004.056 DOI:10.24412/2541-9269-2024-2-18-21

ПОДБОР ПАРАМЕТРОВ ДЛЯ ПОСТРОЕНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ РИСКОВ ВОЗНИКНОВЕНИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ПРЕДПРИЯТИЙ

Ковалёв А.Д.[1]
[1]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, kovalev.ad13@gmail.com

SELECTION OF PARAMETERS FOR BUILDING THE MATHEMATICAL MODEL FOR ASSESSING THE RISKS OF TECHNICAL CHANNELS FOR INFORMATION LEAKAGE AT INFORMATION OBJECTS OF ENTERPRISES

Kovalev A.D.[1]
[1]Yuri Gagarin State Technical University of Saratov, Russia, Saratov, kovalev.ad13@gmail.com

Аннотация. Данная статья представляет исследование по подбору параметров для построения математической модели оценки рисков возникновения технических каналов утечки информации на объектах информатизации предприятий, которые обрабатывают информацию ограниченного распространения. Рассмотрены каналы утечки, возможности средств разведки злоумышленника и выведены параметры для построения математической модели оценки рисков возникновения утечки.

Ключевые слова: математическое моделирование, технические каналы утечки информации, оценка рисков, аппаратура разведки.

Abstract. This article presents a study on the selection of parameters for constructing a mathematical model for assessing the risks of technical channels of information leakage at the facilities of informatization of enterprises that process information of limited distribution. Leakage channels, the capabilities of the attacker's intelligence tools are considered and parameters for constructing a mathematical model for assessing the risks of leakage are derived.

Keywords: mathematical modeling, technical channels of information leakage, risk assessment, intelligence equipment.

В области анализа и оценки рисков информационной безопасности в настоящее время существует несколько методик, работающих с различными параметрами и входными данными, и решающих определенные задачи. Их можно разделить на:

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»);
- количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь);
- методики, использующие смешанные оценки. [1]

Каждая методика имеет свои преимущества и недостатки в построении универсальной модели, поэтому для каждого конкретного случая моделирования системы анализа и оценки рисков могут быть использованы различные подходы. Среди основных систем анализа и оценки рисков можно выделить:

- оценка CRAMM (смешанный подход);
- оценка ГРИФ (смешанный подход);
- оценка RiskWatch (количественный подход);
- оценка CORAS (качественный подход);
- оценка MSAT (качественный подход).[2]

Одним из частных случаев решения проблемы защиты информации на объектах информатизации предприятий является построение и анализ модели угроз. Специалисты по защите, совместно с пользователями системы, углубленно изучают защищаемую информацию, техническую структуру ее обработки, хранения и использования, собирают данные о возможностях злоумышленника на возможных направлениях разведки.

Касаемо, защиты информации от утечки по техническим каналам, как одной из рассматриваемых категорий при построении системы защиты на предприятии, сведений по возможностям злоумышленника в открытых источниках очень мало. Из этого следует, что построение математической модели возможного возникновения риска утечки по техническим каналам, и оценки его на конкретном объекте, маловероятно.

Рассмотрим, каналы утечки информации, обрабатываемой в технических средствах приема, хранения, обработки и передачи информации (ТСПИ):

- побочное электромагнитное излучение элементов, содержащихся в 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. [3]

Согласно данным из открытых источников [4] и характеристик специального приемного устройства PKI2715, используемых для разведки [5], дальность перехвата информации с современных средств вычислительной техники не превышает 50 метров. Однако, если разведка будет вестись при расположении аппаратуры на стационарных постах, дальность может достигать 2000 метров [6]. Что же касается наводок на проводные линии технических средств, дальность ведения разведки тесно связана с расположением технического средства относительно проводных коммуникаций и их выхода за пределы контролируемой зоны. Безопасность в этом случае можно гарантировать, лишь проведя определенные замеры с использованием специализированного оборудования. По данным каналам утекает более 60 % всей информации, для перехвата которой используются технические каналы [7].

К системе заземления также предъявляются требования, при которых расположение заземляющего устройства должно быть проведено на расстоянии большем, чем 10 метров от границы контролируемой зоны во избежание несанкционированного доступа к системе [8]. Препятствовать образованию данного канала утечки следует на моменте создания объекта информатизации, т.е. заложить в техническое задание мероприятия по закрытию канала (расположение контура заземления на определенных расстояниях, использование средств активной защиты информации).

Также, распространенным методом хищения информации является перехват наведенных электромагнитных излучений технических средств на посторонние проводники, находящиеся в непосредственной близости. Соединительные линии вспомогательных технических средств и систем или посторонние проводники являются как бы случайными антеннами, при гальваническом подключении к которым средства разведки ПЭМИН возможен перехват наведенных в них информационных сигналов [9]. В данном случае дальность ведения разведки будет определяться не только уровнем информативного сигнала, но и протяженностью проводника, являющегося антенной.

Нужно понимать, что это исследования, проведенные в специальных лабораториях, и хищение информации с реальных объектов не всегда и не сразу можно заметить и принять определенные действия.

Также, в определенных случаях, необходимо сопоставлять важность защищаемой информации в системе со средствами разведки, т.е. на

предприятие по производству мясной продукции по определенному рецепту, что является защищаемой информацией, с годовым оборотом денежных средств в несколько десятков миллионов рублей не будет вестись разведка техническими средствами, используемыми на стационарных постах и имеющими стоимость, превышающую стоимость разведанной информации в десятки, а то и в сотни, раз.

Важно отметить и достижение требуемого уровня защиты информации. При рассмотрении каналов утечки, связанных с электромагнитными излучениями, провести анализ защищенности без специального оборудование практически невозможно, исключение составляют системы, находящиеся на больших расстояниях от границы контролируемой зоны и не имеющие выхода за ее пределы проводных коммуникаций. Но в современных реалиях, таких объектов слишком мало. И требуемый уровень защиты достигается вложением денежных средств в инструментальный контроль, проводимый специализированными компаниями, пассивная доработка или применение активных средств защиты. А в свою очередь, фото-, видео-, видовая съемки мониторов и других объектов отображения защищаемой информации ТСПИ, может быть исключена организационными мерами, такими как пропускной режим и светоискажение через оконные проемы, что для предприятия не понесет никаких затрат.

Исходя из вышеперечисленного, можно сделать вывод, что следует принимать во внимание такие параметры для оценки и построения математической модели возможного возникновения технических каналов утечки информации, как важность защищаемой информации, приблизительная стоимость оборудования и систем для злоумышленника, и возможные ассигнования в средства защиты.

Литература

1. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 31010:2009. Менеджмент риска. Методы оценки риска
2. Баранова С.Ю. Методики анализа и оценки рисков информационной безопасности, Вестник Московского университета им. С.Ю. Витте. Серия 3. Образовательные ресурсы и технологии, 2015. – № 1(9). – С. 73-79.
3. Зайцев А. П. Технические средства и методы защиты информации. Учебник для вузов/ А. П. Зайцев, А.А. Шелупанов, Р. В. Мещеряков. Под редакцией А. П. Зайцева и А.А. Шелупанова. - 7-е изд., испр. - М.: Горячая линия – Телеком, 2023. - 444 с: ил
4. Хорев А.А. Технические каналы утечки информации, обрабатываемые средствами вычислительной техники // Специальная техника. 2010. № 2 [Электронный ресурс].URL: https://www.vrsystems.ru/stati/texnicheskie_kanali_utechki_informacii_obrabativaemoi_sredstvami_vicislitelnoi_texniki__xorev_aa.htm (дата обращения 21.01.2024)

5. Киреева Н. В. Утечка информации по каналам ПЭМИ и способы их защиты/ Н. В. Киреева, А. В. Семенов/ Международный журнал прикладных и фундаментальных исследований. № 8. 2016. С. 499-504.
6. Гуляев В. П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплект/ В. П. Гуляев. - Екатеринбург: Изд-во Урал. ун-та, 2014.-164 с
7. Способы и средства защиты информации от утечки по техническим каналам // Searchinform. 27.04.2021. URL: http:/searchinform.ru/analitika-v-oblasti-ib/utechki-informacii/sluchai-utechki-informacii/technicheskie-kanali-utechki-informacii/sposoby-i-sredstva-zaschiti-informacii-ot-utechki-po-tehnicheskim-kanalam/ (дата обращения 05.01.2024)
8. Хорев А.А. Способы защиты объектов информатизации от утечки информации по техническим каналам: заземление технических средств обработки информации. Специальная техника. 2012. № 9 [Электронный ресурс].URL: http://www.bnti.ru/showart.asp?aid=995&lvl=04.03. (дата обращения 05.01.2024)
9. Хорев А.А. Технические каналы утечки информации, обрабатываемой техническими средствами//bnti.ru 28.04.2006. [Электронный ресурс]. URL: http://www.bnti.ru/showart.asp?aid=644&lvl=04.02. (дата обращения 05.01.2024)