ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

انتشار الإشعاع الكهرومغناطيسي باعتباره تهديداً لأمن المعلومات لشبكات الشركات

Андрукович Андрей Викторович
أندريه فيكتوروفيتش أندروكوفيتش
Студент УО «БГУИР,»
طالب بجامعة بيلاروسيا الحكومية للاتصالات والمعلوماتية

Буневич Михаил Алексеевич
ميخائيل ألكسيفيتش بونيفيتش
Нау. сотр. лаб. « ММКМ» БГУИР
باحث في مختبر المواد المركبة من أكسيد المعدن متعدد الوظائف بجامعة بيلاروسيا الحكومية للاتصالات والمعلوماتية

Аннотация: *В работе рассматривается проблема утечки информации в корпоративных сетях через побочные электромагнитные излучения. Традиционные методы защиты информации от несанкционированного доступа не учитывают эту угрозу. Установлены закономерности уровня побочных излучений от применяемого типа применяемого кабеля.*

Ключевые слова: побочные электромагнитные излучения, информационная безопасность, компьютерные сети, технические каналы утечки информации

الخلاصة : تتناول الورقة مشكلة تسرب المعلومات في شبكات الشركات من خلال الانبعاثات الكهرومغناطيسية الجانبية. لا تأخذ الطرق التقليدية لحماية المعلومات من الوصول غير المصرح به في الاعتبار هذا التهديد. يتم تحديد انتظام مستوى الإشعاعات العرضية من نوع الكابل المطبق.

الكلمات المفتاحية : الانبعاثات الكهرومغناطيسية الجانبية وأمن المعلومات وشبكات الكمبيوتر والقنوات التقنية لتسريب المعلومات

Введение

Наиболее важным аспектом защиты корпоративных сетей является предотвращение несанкционированного доступа к информации. В традиционных подходах это достигается путем установки брандмауэров, антивирусов и других программных средств защиты информации. Также обеспечивается контроль доступа к телекоммуникационному оборудованию, чтобы снизить риск подключения к сети несанкционированных устройств. Однако, традиционные подходы не включают защиту от утечки информации, циркулирующей в сети, по техническим каналам, в частности, по каналам побочных электромагнитных излучений (далее – ПЭМИ).

Результаты и обсуждение

Для оценки возможности утечки информации, циркулирующей в сети по каналу ПЭМИ был собран стенд, структурная схема которого представлена на рис.1.

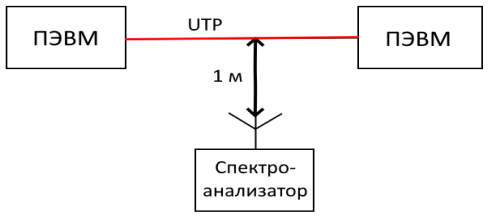

Рис 1. Стенд для обнаружения ПЭМИ от кабеля передачи данных локальной вычислительной сети

Стенд состоит из двух персональных электронных вычислительных машин (далее – ПЭВМ), объединенных в локальную вычислительную сеть (далее – ЛВС) с помощью кабеля с витой парой. Экспериментально было установлено, что при имеющемся оборудовании потеря пакетов начинает происходить при длине кабеля типа UTP (U/UTP по ISO/IEC 11801) [1] 5-го класса в 90 метров.

Для измерения уровня электромагнитного излучения в метре от кабеля был установлен спектроанализатор Agilent E4404B с антенной измерительной АИ5-0. Для исключения влияния на результаты измерений, точка установки спектроанализатора была выбрана на максимальном расстоянии от технических средств обоих ПЭВМ (45 метров). В качестве гарантированной информационной нагрузки на сеть использовалась утилита ping операционной системы Windows.

Изначально при выключенных ПЭВМ был измерен электромагнитный фон на частотах 30, 100, 250 500 МГц. После этого ПЭВМ были включены, на одной из них была запущена утилита ping, проведены измерения уровня электромагнитного излучения на вышеперечисленных частотах.

Описанный эксперимент был повторен для кабелей типов F/UTP, S/UTP, SF/UTP пятого класса. Результаты экспериментов представлены на рис.2.

	30 МГц	100 МГц	250 МГц	500 МГц
Фон, дБ/мкВм	23,43	27,33	24,16	21,46
U/UTP, дБ/мкВм	29,21	32,92	32,27	22,14
F/UTP, дБ/мкВм	29,45	31,69	30,55	20,56
S/UTP, дБ/мкВм	25,34	29,13	28,74	21,48
SF/UTP, дБ/мкВм	24,73	27,95	25,11	22,21

Рис.2. Результаты эксперимента

По полученным данным можно утверждать, что ПЭМИ от кабеля с витой парой были обнаружены. ПЭМИ находится в диапазоне до 500 МГц. Также можно сделать вывод, что на уровень ПЭМИ влияет тип кабеля, применяемого в ЛВС.

Выводы

В ходе работы были проведены эксперименты по выявлению ПЭМИ от информационных линий ЛВС. Разработанный стенд позволил измерить уровень электромагнитного излучения от информационного кабеля с витой парой в макете сегмента корпоративной сети.

Исходя из полученных данных можно сделать вывод, что утечка информации по каналу ПЭМИ является потенциальной угрозой информационной безопасности корпоративной сети.

Таким образом при обеспечении информационной безопасности стоит обращать внимание на типы информационных кабелей, применяемых в корпоративной сети – предпочтительнее использовать кабели с двойным экранированием. Также необходимо ограничить доступ не только к телекоммуникационному оборудованию, но и обеспечить контролируемую зону на всей протяженности прокладки информационного кабеля.

المقدمة

أهم جانب من جوانب حماية شبكات الشركات هو منع الوصول غير المصرح به إلى المعلومات. في النهج التقليدية، يتم تحقيق ذلك من خلال تثبيت جدران الحماية ومكافحة الفيروسات وغيرها من برامج حماية المعلومات. كما يتم التحكم في الوصول إلى معدات الاتصالات السلكية واللاسلكية للحد من مخاطر اتصال الأجهزة غير المصرح بها بالشبكة. ومع ذلك، لا تشمل النُهج التقليدية الحماية من تسرب المعلومات المتداولة في الشبكة من خلال القنوات التقنية، ولا سيما من خلال قنوات الانبعاثات الكهرومغناطيسية الجانبية (المشار إليها فيما يلي - PEMI).

النتائج والمناقشة

لتقييم إمكانية تسرب المعلومات المتداولة في الشبكة من خلال قنوات الانبعاثات الكهرومغناطيسية الجانبية ، تم تجميع حامل، يظهر مخططه الهيكلي في الشكل 1.

الشكل 1. حامل للكشف عن الانبعاثات الكهرومغناطيسية من كابل نقل البيانات للشبكة المحلية.

يتألف الحامل من جهازي حاسوب إلكتروني شخصي (يشار إليهما فيما يلي باسم الحواسيب الشخصية) متصلين بشبكة محلية (يشار إليها فيما يلي باسم الشبكة المحلية) باستخدام كابل زوجي ملتوي. وقد ثبت تجريبيًا أنه مع المعدات المتاحة يبدأ فقدان الحزمة في الحدوث عند طول الكابل من نوع U/UTP) UTP وفقًا لمعيار ISO/IEC 11801) [1] من الفئة الخامسة البالغ 90 مترًا .

لقياس مستوى الإشعاع الكهرومغناطيسي، تم تركيب محلل طيفي Agilent E4404B مزود بهوائي قياس AI5-0 على بعد متر واحد من الكابل. لتجنب التأثير على نتائج القياس، تم اختيار نقطة تركيب المحلل الطيفي على أقصى مسافة من الوسائل التقنية لكلا جهازي الكمبيوتر الشخصي (45 مترًا). تم استخدام الأداة المساعدة ping الخاصة بنظام التشغيل ويندوز كحمل معلومات مضمون على الشبكة .

في البداية، تم قياس الخلفية الكهرومغناطيسية عند الترددات 30، 100، 250، 500 ميجاهرتز عند إيقاف تشغيل أجهزة الكمبيوتر الشخصي. بعد ذلك تم تشغيل أجهزة الكمبيوتر، وتم تشغيل أداة ping على أحدها وتم إجراء قياسات لمستوى الإشعاع الكهرومغناطيسي عند الترددات المذكورة أعلاه.

تم تكرار التجربة الموصوفة لكابلات من أنواع F/UTP و S/UTP وSF/UTP من الفئة الخامسة. وترد نتائج التجارب في الشكل 2.

	30 МГц	100 МГц	250 МГц	500 МГц
Фон, дБ/мкВм	23,43	27,33	24,16	21,46
U/UTP, дБ/мкВм	29,21	32,92	32,27	22,14
F/UTP, дБ/мкВм	29,45	31,69	30,55	20,56
S/UTP, дБ/мкВм	25,34	29,13	28,74	21,48
SF/UTP, дБ/мкВм	24,73	27,95	25,11	22,21

الشكل 2. النتائج التجريبية

ووفقًا للبيانات التي تم الحصول عليها، يمكن القول إنه تم الكشف عن وجود PEMI من كابل زوجي ملتوي. يصل مستوى PEMI إلى 500 ميجاهرتز. يمكن أيضًا استنتاج أن مستوى PEMI يتأثر بنوع الكابل المستخدم في الشبكة المحلية.

الخاتمة

في سياق العمل تم إجراء تجارب للكشف عن الإشعاع الكهرومغناطيسي من خطوط معلومات الشبكة المحلية. وقد مكّن الحامل المطور من قياس مستوى الإشعاع الكهرومغناطيسي من كابل المعلومات المزدوج الملتوي في نموذج قطاع شبكة الشركة.

واستناداً إلى البيانات التي تم الحصول عليها، يمكننا أن نستنتج أن تسرب المعلومات من خلال قناة PEMI يشكل تهديداً محتملاً لأمن المعلومات في شبكة الشركة .

وبالتالي، عند ضمان أمن المعلومات، يجدر الانتباه إلى أنواع الكابلات المعلوماتية المستخدمة في شبكة الشركة - يفضل استخدام الكابلات ذات التدريع المزدوج. ومن الضروري أيضًا تقييد الوصول ليس فقط إلى معدات الاتصالات السلكية واللاسلكية، ولكن أيضًا لتوفير منطقة محكومة على طول طول كابل المعلومات الممتد.

References المراجع والمصادر

1. ISO/IEC 11801-1:2017. Information technology. Generic cabling for customer premises. Part 1: General requirements