Keamanan Informasi Sintesis Sistem
Menggunakan Teori Grafik

VN Kustov, VV Yakovlev, TL Stankevich
Universitas Kaisar Alexander I St. Petersburg State Transport
Petersburg, Rusia

Abstrak **pencegahan --Timely ancaman keamanan informasi, disediakan oleh perangkat lunak khusus dan perangkat keras, adalah dasar bisnis yang efektif, yang memungkinkan untuk mengurangi risiko reputasi dan keuangan bagi perusahaan. Pada saat yang sama, perlindungan harus diterapkan di semua pengkritik kemungkinan serangan area. Jika kita beralih ke Federasi Rusia IeISSlation, maka urutan FSTEC №31 dari 14 Maret 2014 dapat diadopsi sebagai dasar untuk "mengisolasi" vektor-vektor perlindungan, yang menurut langkah-langkah dasar untuk perlindungan harus disediakan di tingkat berikut: akses identifikasi pelajaran dan otentikasi, akses delineasi, pembatasan perangkat lunak, media penyimpanan komputer perlindungan, dll (Ada 21 dari mereka). Pada perangkat keras dan perangkat lunak yang kompleks dasar yang menerapkan perlindungan di masing-masing tingkat, sistem keamanan informasi perusahaan dibuat. Untuk memilih keamanan perangkat lunak dan perangkat keras informasi yang paling tepat, dan, karena itu, untuk membangun sistem perlindungan informasi perusahaan yang optimal, seseorang dapat beralih ke grafik teori. Dalam hal ini, masalah berkurang untuk konstruksi grafik menurun yang peringkat dan solusi masalah optimalitas, yaitu kritis (maksimal) jalan grafik calculation ini. Setiap tingkat grafik sesuai dengan subsistem khusus dari sistem keamanan informasi, sedangkan subsistem terletak di dugaan perlindungan agar mengatasi oleh penyerang; puncak - alat keamanan informasi dipertimbangkan; grafik tertimbang,**

Kata kunci - solusi masalah optimalitas atas dasar teori grafik; grafik jalur kritis; sintesis sistem keamanan informasi berdasarkan teori grafik; keamanan informasi perusahaan

Tepat waktu ancaman keamanan informasi pencegahan serta penghapusan menyadari konsekuensi ancaman yang cepat adalah basis bisnis yang efektif. Pada saat yang sama, perlindungan harus diterapkan di semua pengkritik mungkin daerah serangan.

Jika kita beralih ke Federasi Rusia IeISSlation, maka urutan FSTEC №31 dari 14 Maret 2014 dapat diadopsi sebagai dasar untuk “mengisolasi” vektor-vektor perlindungan, yang menurut langkah-langkah dasar untuk perlindungan harus diberikan pada berikut tingkat : mengakses entitas identifikasi dan otentikasi, akses batas, pembatasan perangkat lunak, penyimpanan komputer perlindungan media, peristiwa keamanan merekam, perlindungan antivirus, Deteksi gangguan (pencegahan), pemantauan keamanan informasi, informasi otomatis integritas sistem manajemen, sarana teknis dan ketersediaan informasi, lingkungan virtualisasi perlindungan, hardware dan peralatan perlindungan, sistem otomatis dan perlindungan komponen, pengembangan aman dan perangkat lunak manajemen, manajemen pembaruan perangkat lunak, informasi perencanaan keamanan, penyediaan tindakan kontingensi, informasi personil dan pelatihan, analisis informasi dan risiko dari mereka penerapan, deteksi insiden dan respon, manajemen konfigurasi sistem manajemen otomatis dan sistem perlindungan. Dengan demikian, jumlah tingkat yang perlindungan dari penyerang internal dan eksternal harus dilaksanakan adalah 21 atau 21 subsistem dari sistem keamanan informasi (ISS).

Untuk memilih alat-alat keamanan informasi yang paling tepat (dari keamanan yang diperlukan posisi tingkat dan kemampuan materi yang tersedia), dan, akibatnya, perusahaan ISS konstruksi yang optimal, seseorang dapat beralih ke grafik teori. Dalam hal ini, masalah berkurang untuk membangun grafik menurun peringkat dan memecahkan masalah optimasi, yaitu grafik perhitungan kritis (maksimal) jalan ini. Setiap tingkat grafik sesuai dengan subsistem tertentu ISS, sedangkan subsistem berada dalam perlindungan dugaan mengatasi rangka oleh penyerang; simpul - Informasi sarana keamanan yang diadopsi untuk perbandingan; grafik tertimbang, masing-masing berat busur yang sesuai dengan preferensi untuk menggunakan ahli evaluasi alat tertentu.

I. MODEL ANCAMAN DAN PENGEMBANGAN MODEL INTRUDER

Sebagai ISS sintesis tahap persiapan menggunakan teori graph, kita membedakan model ancaman dan tahap pengembangan model penyusup [1].

Ketika Model penyusup berkembang, kita tidak boleh lupa bahwa regulator informasi utama pendekatan bidang keamanan kami, tetap dalam dokumen (Metode) disetujui oleh mereka, berbeda dalam masalah ini. Rusia Dinas Keamanan Federal (FSS) bertanggung jawab untuk regulasi bidang kriptografi, dan metodologi disetujui oleh menggambarkan penyusup dalam menyerang kemampuan kripto [2]. Rusia Layanan Federal untuk Teknis dan Ekspor Control (FSTEC) [3] adalah lebih luas dan menggambarkan kemampuan pelaku untuk menyerang sistem secara keseluruhan.

FSS dan FSTEC pendekatan dapat diintegrasikan sebagai berikut:

- rendah penyusup potensial di bawah FSTEC adalah penyusup H1-H3 menurut klasifikasi FSS;
- Rata-rata potensi penyusup di bawah FSTEC adalah penyusup H4-H5 menurut klasifikasi FSS;
- penyusup potensial tinggi di bawah FSTEC adalah penyusup H6 menurut klasifikasi FSS.

978-1-5386-1810-3 / 17 / $ 31.00 © 2017 IEEE

Selanjutnya, berdasarkan kelas sistem informasi, kita memilih jenis penyusup dari mana kita perlu mempertahankan diri.

Jika sistem perusahaan diklasifikasikan sebagai sistem informasi negara, Anda harus merujuk pada klausul 25 dari FSTEC Orde No 17 [4]:

- untuk sistem informasi keamanan kelas - ancaman netralisasi dari penyusup dengan potensi tinggi;
- untuk sistem informasi keamanan kelas dua - ancaman netralisasi dari penyusup dengan potensi rata-rata;
- untuk sistem informasi keamanan ketiga dan keempat kelas - ancaman netralisasi dari penyusup dengan potensi rendah.

Dalam hal sistem tidak jatuh ke dalam kategori negara, perlu untuk mengubah Keputusan Pemerintah Nomor 1119 [5]:

- pertama jenis ancaman terkait dengan kemampuan dideklarasikan di hadapan sistem software - ancaman netralisasi dari penyusup dengan potensi tinggi;
- jenis ancaman kedua terkait dengan kemampuan dideklarasikan di hadapan perangkat lunak sistem - ancaman netralisasi dari penyusup dengan potensi menengah;
- jenis ancaman ketiga terkait dengan kemampuan dideklarasikan dalam perangkat lunak sistem kehadiran - ancaman netralisasi dari penyusup dengan potensi rendah.

Dalam tahap ini, sistem informasi perusahaan tingkat keamanan awal (sebelum pelaksanaan ISS) juga ditentukan, yang diperlukan untuk mengkompilasi daftar ancaman keamanan informasi aktual (Tabel I) .

TABEL I. saya NITIAL KEAMANAN TINGKAT PENENTUAN

karakteristik teknis dan operasional	Tingkat keamanan
tempat	Rendah sedang Tinggi
sistem informasi sarana teknis lokasi mengenai batas-batas zona dikendalikan	Rendah sedang Tinggi
Kehadiran koneksi dengan sistem informasi lainnya	Rendah sedang Tinggi
Kehadiran koneksi ke Internet	Rendah sedang Tinggi
Built-in (hukum) operasi dengan catatan database	Rendah sedang Tinggi
Pada modus pengolahan informasi	Rendah sedang Tinggi
ketersediaan akses informasi	Rendah sedang Tinggi
alam akses ke informasi	Rendah sedang Tinggi
Menurut alam software diterapkan untuk memproses informasi	Rendah sedang Tinggi

Perlindungan tingkat awal didefinisikan sebagai berikut:

1. Sistem informasi memiliki awal tingkat tinggi keamanan, jika setidaknya 70% karakteristik sesuai dengan tingkat “tinggi” (keputusan positif pada kolom kedua sesuai dengan keamanan yang tinggi tingkat dirangkum), dan sisanya ke tingkat keamanan rata-rata (keputusan positif untuk kolom ketiga).

2. Sistem informasi memiliki keamanan awal tingkat rata-rata jika kondisi untuk item 1 tidak terpenuhi dan setidaknya 70% karakteristik sesuai dengan tingkat tidak lebih rendah dari “rata-rata” (positif keputusan rasio jumlah untuk kolom ketiga sesuai dengan tingkat keamanan rata-rata untuk keputusan jumlah diambil), dan sisanya - tingkat keamanan rendah.

3. Sistem informasi memiliki rendah tingkat keamanan awal jika kondisi untuk item 1 dan 2 tidak terpenuhi.

Ketika menyusun masing-masing tingkat keamanan awal ancaman keamanan yang sebenarnya dalam daftar sistem informasi, koefisien numerik (Y1) dimasukkan dalam korespondensi, yaitu :

0 - untuk keamanan awal tingkat tinggi ; 5 - untuk keamanan awal gelar rata-rata ; 10 - untuk keamanan awal tingkat rendah .

Probabilitas realisasi ancaman dipahami sebagai indikator ahli ditentukan mencirikan bagaimana mungkin adalah implementasi ancaman khusus untuk keamanan informasi untuk sistem informasi perusahaan dalam kondisi yang muncul .

The numerik koefisien (Y2) untuk menilai probabilitas ancaman terjadinya ditentukan oleh 4 gradasi lisan indikator ini :

- tidak mungkin - tidak ada prasyarat obyektif untuk pelaksanaan ancaman (Y2 = 0);
- probabilitas rendah - prasyarat obyektif untuk pelaksanaan ancaman ada, tetapi kebijakan yang diambil membuatnya sangat sulit untuk menerapkannya (Y2 = 2);
- Rata-rata probabilitas - prasyarat obyektif untuk pelaksanaan ancaman ada, tetapi langkah-langkah keamanan yang diambil tidak mencukupi (Y2 = 5);
- probabilitas tinggi - prasyarat obyektif untuk pelaksanaan ancaman yang ada dan langkah-langkah keamanan tidak diambil (Y2 = 10).

Berdasarkan evaluasi tingkat keamanan (Y1) dan ancaman probabilitas (Y2), faktor ancaman realisasinya (Y) adalah dihitung dan ancaman realisasi kemungkinan ditentukan. Faktor ancaman direalisasi Y akan ditentukan oleh relasi $Y = (Y_1 + Y_2) / 20$.

Keamanan informasi penilaian ancaman bahaya didasarkan pada penilaian ahli dan ditentukan oleh indikator bahaya verbal yang memiliki tiga makna :

- risiko rendah - jika pelaksanaan ancaman dapat menyebabkan konsekuensi negatif kecil;
- bahaya menengah - jika pelaksanaan ancaman dapat menyebabkan konsekuensi negatif;
- bahaya tinggi - jika pelaksanaan ancaman dapat mengakibatkan konsekuensi negatif yang signifikan.

Sesuai dengan menugaskan para aturan ancaman keamanan terhadap sebenarnya (Tabel II), sistem informasi perusahaan itu menentukan ancaman aktual dan relevan .

TABEL II. R Ules UNTUK MENENTUKAN ANCAMAN URGENSI

realisasi ancaman kemungkinan	indikator ancaman		
	Rendah	***Medium***	*Tinggi*
Rendah	tidak relevan	tidak relevan	Sebenarnya
Medium	tidak relevan	Sebenarnya	Sebenarnya
Tinggi	Sebenarnya	Sebenarnya	Sebenarnya
Sangat tinggi	Sebenarnya	Sebenarnya	Sebenarnya

Memiliki didefinisikan kategori sistem informasi dan kelas, memiliki ancaman dan penyusup model, mengetahui daftar tingkat (subsistem) yang perlu untuk memberikan perlindungan dari penyerang, Anda dapat melanjutkan ke software, hardware dan pasar firmware analisis, dan memilih dari keseluruhan berbagai optimal

hanya untuk kami untuk harga, kualitas dan fungsionalitas.

II. S OFTWARE DAN HARDWARE SELEKSI UNTUK SETIAP ISS SUBSYSTEM

Seperti yang telah ditentukan sebelumnya, perlindungan informasi harus dilaksanakan pada 21 tingkat, sedangkan tingkat berada dalam perlindungan dugaan mengatasi rangka oleh penyerang. Perlindungan pada setiap tingkat disediakan oleh alat khusus, yang pada gilirannya adalah masa depan peringkat bawah grafik vertex.

Berdasarkan persyaratan untuk fungsi yang ditugaskan untuk perangkat tertentu, serta kemampuan perusahaan bahan, ahli memilih dana yang disajikan di pasar, menentukan prioritas dalam menggunakan satu atau yang lain. prioritas akan sesuai dengan berat busur .

Dengan demikian, kita telah membangun grafik top-down peringkat di mana simpul adalah alat keamanan informasi ahli terletak pada tingkat tertentu (subsistem), yang pada gilirannya sistematis dalam perlindungan dugaan agar pelanggaran penyerang, dan simpul dihubungkan oleh busur, bobot setiap ditentukan oleh prioritas dalam transisi ke titik ini (Gambar. 1) .

Faktor-faktor bobot ditugaskan untuk busur dapat menjadi berikut (diberikan sebagai contoh, nilai-nilai dapat diubah, daftar diperluas atau disingkat) :

2 - prioritas integrasi rendah ke dalam sistem informasi; 4 - prioritas integrasi rata ke dalam sistem informasi; 6 - prioritas integrasi yang tinggi ke dalam sistem informasi; 1 - busur melakukan fungsi pelayanan (misalnya, transisi dari satu subsistem ISS ke yang berikutnya di balik itu).

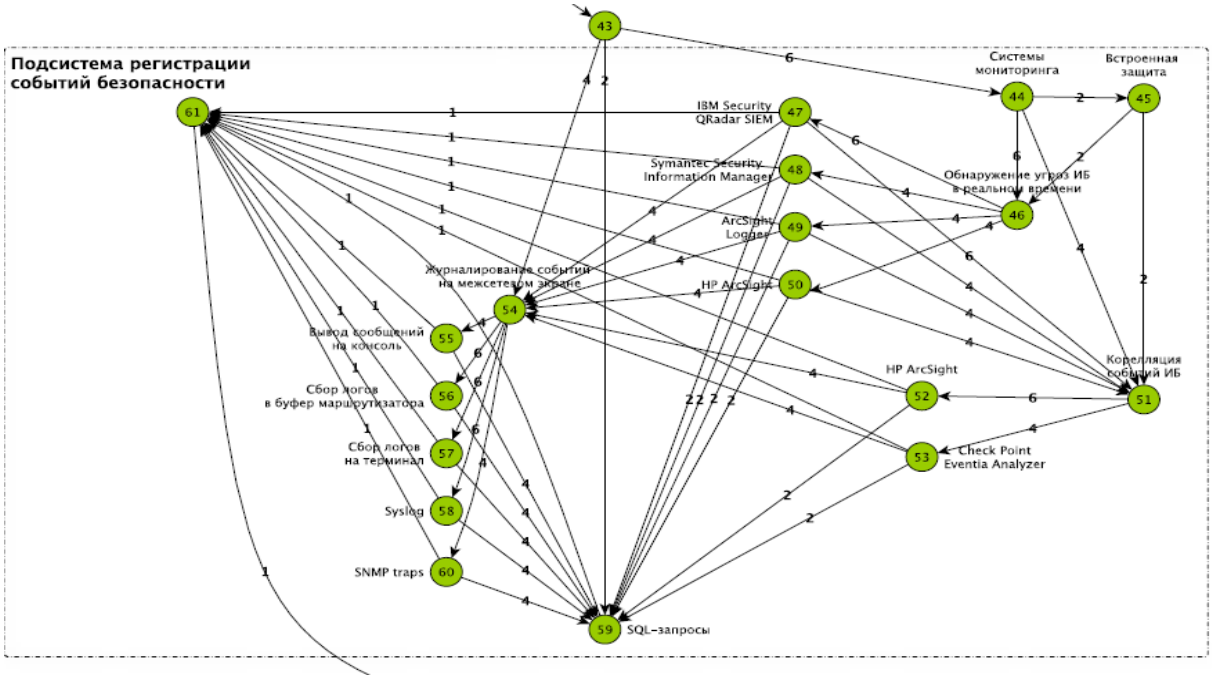
AKU AKU AKU. D ETERMINING THE C RITICAL P ATH OF AG Raph

Menurut grafik dibangun, jalur kritis dengan semua busur bobot nilai maksimum dihitung ketika mengikuti dari grafik awal (sumber) vertex ke final (sink). jalur kritis ini akan sesuai dengan perusahaan yang optimal ISS.

Pada gilirannya, proses jalur menghitung kritis dapat otomatis dengan mengembangkan modul software komputasi sederhana .

IV. C ONCLUSION

Itu pendekatan yang diusulkan untuk perusahaan ISS sintesis adalah padat karya dan membutuhkan para ahli berkualitas tinggi Keterlibatan, tapi perencanaan rinci tersebut dan peramalan akan membantu untuk menghindari pemborosan bahan yang tidak perlu di hari ini dan kerugian finansial yang signifikan dalam hal ancaman keamanan informasi masa depan.



Gambar. 1. peringkat tingkat grafik menurun yang sesuai dengan peristiwa keamanan reISStration subsistem

R EFERENCES

[1] Ancaman model dasar untuk keamanan data pribadi saat memproses mereka dalam sistem informasi data pribadi (ekstrak): officer.text. Moskow: FSTEC Rusia, 2008. 69p [2] metodologis rekomendasi untuk tindakan hukum peraturan pembangunan yang menentukan ancaman terhadap data pribadi keamanan yang relevan untuk pengolahan data pribadi dalam sistem informasi data pribadi dioperasikan dalam kegiatan yang relevan melakukan, disetujui 8 manajemen Pusat Rusia FSS pada 31 Maret 2015 No. 149/7/2 / 6-432. Moskow.: 2015. 22p.

[3] Mengidentifikasi ancaman metodologi untuk keamanan informasi dalam sistem informasi (Proyek). Moskow: Rusia FSTEC 2015. 43p. [4] Urutan Rusia FSTEC tanggal 11 Februari 2013. № 17 “Di persetujuan persyaratan untuk keamanan informasi yang tidak rahasia negara, yang terkandung dalam sistem informasi pemerintah”[sumber daya Elektronik]. - Akses modus: http://fstec.ru (tanggal sirkulasi 2017/07/04). [5] Rusia Resolusi Pemerintah Nomor 1119 tanggal 2012/01/11 "Pada menyetujui persyaratan untuk perlindungan data pribadi saat memproses mereka dalam sistem informasi data pribadi"[sumber daya Elektronik]. - Mode akses: http://consultant.ru (tanggal sirkulasi 2017/07/04).