# Manajemen Risiko dalam Sistem Keamanan

*Abstract*— Manajemen dan manajemen risiko keamanan adalah bagian dari pemerintahan umum negara, dan oleh karena itu tidak mungkin untuk memeriksanya secara terpisah dan bahkan jika itu, satu pemeriksaan terpisah tidak akan memberi kita gambaran lengkap tentang bagaimana menerapkan proses ini. Pemahaman modern tentang manajemen keamanan strategis tidak hanya membutuhkan upaya terus-menerus untuk meningkatkan pembentukan dan implementasi kebijakan keamanan tetapi juga pendekatan baru dan solusi khusus untuk memodernisasi sistem keamanan dengan membuatnya memadai untuk persyaratan lingkungan keamanan yang dinamis [1]. proses manajemen risiko keamanan informasi menggunakan model fungsional dan kontekstual yang mencerminkan konsep dasar dan fungsi dasar sistem manajemen risiko keamanan informasi. pengembangan sistem manajemen risiko adalah tugas penting dari keseluruhan masalah untuk memastikan keamanan informasi. [4]

. *Kata kunci* — keamanan, manajemen, risiko, manajemen

Lingkungan keamanan modern dan karakteristik dasarnya - prediksi yang sangat sulit dan dapat diperkirakan sebelumnya menegaskan proses penciptaan keterampilan yang diperlukan angkatan bersenjata sebagai respons yang paling memadai terhadap kebutuhan adaptasi yang berkelanjutan dan peningkatan keterampilan mereka. Mempercepat munculnya pengetahuan baru, inovasi dan memajukan penelitian melalui penelitian yang berkaitan dengan keamanan, menghasilkan pengetahuan baru dan mempromosikan implementasi teknologi baru di bidang keamanan masyarakat.

Risiko memahami kemungkinan timbulnya salah satu peristiwa yang mungkin terjadi, menimbulkan berbagai kerugian. Isu memastikan keamanan informasi aplikasi sekarang menjadi sangat penting. Melakukan penilaian risiko kualitatif dan tepat waktu, serta mempelajari masalah pengelolaannya dan metode untuk meminimalkannya dari yang sebenarnya dan populer di masyarakat informasi modern. Pendekatan sistematis untuk analisis risiko memungkinkan penyelesaian masalah di bidang cybersecurity dan menciptakan yang efektif [2]

Mengumpulkan pengetahuan keamanan dengan mengubah penemuan menjadi suatu produk menciptakan potensi yang sangat besar, tetapi itu tidak cukup untuk menjadi pengetahuan yang berguna dan bermanfaat. Hubungan antara pembangunan ekonomi dan pengetahuan ilmiah secara jelas menunjukkan kepada kita perlunya pengalaman dan keterampilan agar dapat diproses dan digunakan. Hal ini membutuhkan teori dan praktik untuk menggunakan istilah "ekonomi baru", yang sumber daya yang menentukannya adalah pengetahuan dan manajemennya, karena tidak mungkin untuk melakukan hal itu, yang belum memiliki pengetahuan yang diperlukan.

Keamanan nasional masyarakat modern adalah baik dan suatu keharusan di mana keamanan harus dianggap sebagai kegiatan ekonomi. Pendekatan untuk pengembangannya, pengambilan dan penerapan keputusan manajemen tidak berbeda dari organisasi bisnis, dan efek dari transformasi sumber daya yang diinvestasikan dalam keamanan memiliki tujuan akhir untuk mencapai tujuan yang ditetapkan untuk angkatan bersenjata

Berbagi informasi keamanan secara terus-menerus, memberikan kesadaran situasional keseluruhan tentang status keamanan , serta dasar untuk mengidentifikasi ancaman melalui korelasi yang diperluas dari insiden yang terisolasi;

• Sarana untuk mendukung resolusi krisis keamanan, meminimalkan gangguan dan dampak terhadap sistem secara keseluruhan

• Peningkatan kemampuan (operasional dan teknologi) untuk menghadapi ancaman yang muncul. [3]

Sistem keamanan adalah organisasi yang berorientasi misi yang memiliki sifat kuat, integritas dan konektivitas dengan semua sektor publik, yang juga menentukan kekhususan manajemen keamanan strategis. Tujuan utama dari keamanan strategis manajemen adalah membangun dan mempertahankan kemampuan defensif untuk mengendalikan ancaman dan risiko bagi masyarakat dalam batas yang dapat diterima.

Dengan kekuatan imperatif, kebutuhan implementasi manajemen ilmiah dan manajemen perubahan, sementara menghormati persyaratan efisiensi dan transparansi dalam sistem keamanan, memerlukan tanggung jawab yang sesuai dengan kewajiban dan kemampuan beradaptasi terhadap perubahan dalam lingkungan keamanan, risiko dan tantangan. Membangun keamanan berbasis pengetahuan adalah masalah, tetapi juga merupakan tantangan bagi tim dalam organisasi pendidikan sains di sektor keamanan. Manajemen strategis di dalamnya adalah paradigma yang memungkinkan mereka melalui kekuatan pengetahuan ilmiah untuk mengubah peran mereka dalam menciptakan sektor keamanan nasional terpadu di masa depan yang berkontribusi pada "keamanan cerdas" negara.

Manajemen keamanan strategis menyiratkan pemikiran strategis luas dengan visi masa depan yang jelas dan melibatkan merumuskan, mengimplementasikan, dan mengevaluasi solusi yang memungkinkan untuk mencapai tujuan utama kebijakan keamanan - untuk menciptakan lingkungan yang kondusif bagi realisasi kepentingan nasional melalui penciptaan, pengembangan , dan penggunaan kemampuan sistem keamanan jika ada ancaman dan risiko yang masuk akal. Pemilihan strategi pemenang dari organisasi tergantung pada tekanan strategis dan biaya (manfaat) yang diinginkannya; ancaman yang dihadapinya dalam aktivitasnya dan peluang yang ingin ia manfaatkan melaluinya. Keamanan adalah salah satu kebutuhan dasar individu dan kelompok yang menonjol terlepas dari harga.

Semua perubahan ini terkait dengan ketidakpastian dan risiko - perubahan tersebut semakin baru, belum dijelajahi, dan kompleks, yang beragam terkait dengan pengembangan teknologi, proses globalisasi dan transformasi regional, hubungan internasional, dll., Yang pada gilirannya menyiratkan bahwa risiko untuk dikelola oleh pendekatan inovatif dan tidak konvensional yang memperlakukannya sebagai bagian integral dari proses manajemen umum kegiatan organisasi.

Manajemen risiko, sebagai bagian dari manajemen keamanan strategis, berfokus pada identifikasi risiko dan pendekatan definisi untuk mengurangi dampaknya dalam hal tujuan pengaturan, persyaratan sumber daya untuk pencapaian tujuan, perubahan dalam lingkungan - eksternal dan internal, dan terakhir, keadaan bahwa setiap tujuan diarahkan untuk hasil alternatif di masa depan.

Faktanya, dunia global yang modern telah memasuki era integrasi strategis, penciptaan sistem terintegrasi dan pembangunan model terintegrasi. yang berkontribusi pada pengembangan intensif integrasi sistem dan teknologi pemodelan terintegrasi, karena model yang diberikan adalah yang terbaik untuk mencerminkan interaksi elemen struktural utama dan komponen sistem dan fungsional serta arah targetnya. [5].

Kepatuhan dengan tren saat ini dalam pengembangan sains, dan khususnya sifat interdisipliner penelitian terapan dan penetrasi ke semua cabang ilmu komputer lainnya untuk mengumpulkan, memproses, mengirim dan menyimpan informasi, akan menjadi dasar bagi keberhasilan manajemen organisasi dalam sistem keamanan.

Menerapkan pendekatan sistematis dan proses untuk mengklarifikasi keteraturan dan prinsip-prinsip dasar dari proses manajemen strategis secara paralel paralel untuk hubungan antara teori sosial dan ekonomi, dengan menganalisis definisi, gagasan dasar dan istilah, prinsip, spesifik dan isi proses dalam sistem keamanan, memungkinkan persatuan mereka terungkap dengan logika umum pemikiran strategis dan pengembangan strategis.Hal ini meningkatkan beban kerja untuk mengidentifikasi, menilai, dan mengelola risiko keamanan akibat pencemaran, dan setelah setiap perubahan. Selain risiko keamanan, perubahan juga mengakumulasi utang teknis, sebuah alegori untuk pekerjaan yang ditunda atau dilakukan secara kurang optimal. [6]

Pendekatan arsitektural membentuk dasar teoretis dari teknologi perubahan modern sebagai sains, mempelajari struktur, metode, dan sifat perilaku strategis dalam sistem keamanan. Sebuah alternatif untuk pendekatan untuk memperoleh pengetahuan baru dalam sistem keamanan adalah dengan melakukan penilaian ulang yang terperinci dari set variabel pengendali yang ada sebagai hasil dari ketidakpuasan dengan hasil akhir yang dihasilkan. Tinjauan variabel-variabel baru yang ada dan yang diusulkan membutuhkan perubahan dalam strategi yang diterapkan di mana pencarian dan penghapusan kesalahan (pembelajaran) dalam organisasi (sistem) berada dalam "dua putaran pembelajaran" - dari mengubah variabel yang dapat dikelola hingga memilih strategi yang tepat dan kerangka kerja untuk variabel pelaporan.

Pendekatan analitik dalam penelitian ini memungkinkan pertimbangan integritas interpretasi militer yang sempit tentang manajemen strategis sebagai elemen hubungan sosial ekonomi dan hubungan proses dengan fungsi manajerial lainnya dalam aspek yang jauh lebih luas, dengan mempertimbangkan karakteristik dinamis dari lingkungan keamanan, dengan memperhatikan salah satu tantangan utama bagi manajemen keamanan strategis.

## KESIMPULAN

Ini didasarkan pada penetapan tujuan, ketergantungan sumber daya untuk pencapaian tujuan, perubahan dalam lingkungan - eksternal dan internal, dan terakhir namun tidak kalah pentingnya, harus diperhitungkan bahwa setiap tujuan ditujukan untuk hasil alternatif di masa depan. Sepanjang proses ini, pertanyaannya adalah "bagaimana - jika", yang tanggapannya tidak langsung tetapi ditentukan oleh tindakan yang mungkin, kondisi lingkungan yang memungkinkan dan kemungkinan hasil untuk sistem keamanan.

Kebutuhan obyektif dari proses ini adalah identifikasi situasi risiko yang dihasilkan dari perubahan dalam lingkungan keamanan, kemungkinan untuk terjadinya atau tidak terulangnya, penilaian konsekuensi mereka dan pengambilan keputusan manajemen yang beralasan untuk mengatasi dan pencapaian mereka. dari tujuan yang ditetapkan oleh sistem keamanan. Oleh karena itu, manajemen risiko dipandang sebagai bentuk tata kelola yang diarahkan ke tujuan organisasi keamanan

## REFERENCE


[1] S. Stoykov, “Risk management as a strategic management element in the security system,” *Int. Conf. Creat. Bus. Smart Sustain. Growth, CreBUS 2019*, pp. 1–4, 2019, doi: 10.1109/CREBUS.2019.8840098.

[2] P. N. Anatoliy, F. K. Yuri, D. G. Vagiz, V. K. Yana, and V. S. Aleksandr, “Aggregation process for implementation of application security management based on risk assessment,” *Proc. 2018 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2018*, vol. 2018-January, pp. 98–101, 2018, doi: 10.1109/EIConRus.2018.8317039.

[3] C. Porretti, D. Kolev, and R. Lahaije, “A new vision for ATM security management the security management platform,” *Proc. - 2016 11th Int. Conf. Availability, Reliab. Secur. ARES 2016*, pp. 493–498, 2016, doi: 10.1109/ARES.2016.50.

[4] V. G. Semin, E. G. Shmakova, and A. B. Los, “The information security risk management,” *Proc. 2017 Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2017*, pp. 106–109, 2017, doi: 10.1109/ITMQIS.2017.8085774.

[5] L. Slipachuk, S. Toliupa, and V. Nakonechnyi, “The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine,” *2019 3rd Int. Conf. Adv. Inf. Commun. Technol. AICT 2019 -*

*Proc.*, pp. 451–454, 2019, doi: 10.1109/AIACT.2019.8847877.

[6] K. Rindell and J. Holvitie, “Security risk assessment and management as technical debt,” *2019 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2019*, pp. 1–8, 2019, doi: 10.1109/CyberSecPODS.2019.8885100.