**Universitatea de Stat din Moldova**

**FACULTATEA RELAŢII INTERNAŢIONALE, ŞTIINŢE POLITICE ŞI ADMINISTRATIVE**

**DEPARTAMENTUL RELAŢII INTERNAŢIONALE**

***Tema:***

*"Cadrul de cooperare pe arena internațională în domeniul securității informațiilor și al cooperării între organizațiile internaționale"*

**Autor:Demidenco Vlada**

**Coordonator:Tatiana Busuncian**

**Dr., lector universitar**

**Chişinău, 2023**

**Cuprins**

[**Introducere** 3](#_Toc150587922)

[**Definiție a securității informațiilor** 4](#_Toc150587923)

[**Rolul ONU, NATO și alte organizații în promovarea securității informațiilor** 6](#_Toc150587924)

[**Republica Moldova și cooperare internațională** 9](#_Toc150587925)

[**Concluzii și recomandări** 11](#_Toc150587926)

[**Bibliografie** 13](#_Toc150587927)

# **Introducere**

În era digitală în care tehnologia definește tot mai mult modul în care trăim, lucrăm și interacționăm, securitatea informațiilor devine un pilon esențial al stabilității și prosperității societății moderne. Informațiile, de la datele personale la secretele de stat, sunt activul fundamental al acestei epoci tehnologice, iar protejarea lor devine o provocare complexă și imperativă. În lumina amenințărilor cibernetice tot mai sofisticate, a spionajului digital și a vulnerabilităților tehnologice în continuă evoluție, abordarea securității informațiilor nu este doar o necesitate, ci și o responsabilitate strategică. Această lucrare explorează profunzimea și amplitudinea conceptului de securitate a informațiilor, examinând amenințările actuale, strategiile de protecție, precum și implicarea crucială a factorilor umani și tehnologici în asigurarea unui mediu informațional sigur și încrezător pentru societatea contemporană.

Cadrul de cooperare pe arena internațională în domeniul securității informațiilor și al cooperării între organizațiile internaționale este esențial pentru abordarea amenințărilor cibernetice și a altor aspecte legate de securitatea informațiilor la nivel global. Acest cadru poate include acorduri bilaterale sau multilaterale, precum și organizații internaționale dedicate securității cibernetice, precum INTERPOL, NATO, sau alte organizații cu mandate relevante. Coordonarea și schimbul de informații între state și organizații joacă un rol crucial în prevenirea și contracararea atacurilor cibernetice și în promovarea unei securități cibernetice mai robuste la nivel mondial

Securitatea informațiilor reprezintă un imperativ strategic la nivel global. Cu tehnologii avansate care transformă rapid modul în care comunicăm, interacționăm și gestionăm informațiile, amenințările cibernetice devin tot mai sofisticate și transcind granițele naționale. În acest context, analizarea cadrului de cooperare pe arena internațională în domeniul securității informațiilor și a colaborării între organizațiile internaționale devine esențială pentru protejarea infrastructurii critice, prevenirea atacurilor cibernetice și gestionarea riscurilor asociate. Această lucrare explorează evoluția, importanța și viitorul cooperării internaționale în securitatea informațională, evidențiind aspecte cheie precum schimbul de informații, normele internaționale, amenințările emergente și necesitatea unei acțiuni concertate pentru a asigura un mediu digital sigur și rezilient la nivel mondial.

# **Definiție a securității informațiilor**

Securitatea informațiilor se referă la protejarea datelor, informațiilor și resurselor informatice împotriva accesului neautorizat, divulgării sau distrugerii acestora. Scopul principal al securității informațiilor este asigurarea confidențialității, integrității și disponibilității acestora, precum și prevenirea amenințărilor și atacurilor cibernetice care ar putea compromite aceste aspecte. Aceasta implică implementarea măsurilor de securitate, cum ar fi criptarea datelor, autentificarea utilizatorilor, monitorizarea și gestionarea riscurilor, pentru a proteja informațiile împotriva posibilelor amenințări și vulnerabilități.

Cooperarea internațională în domeniul securității informațiilor este de o importanță crucială în era digitală actuală. Iată câteva motive cheie:

1. Amenințările cibernetice nu cunosc granițe: Amenințările cibernetice nu cunosc granițe

2. Resurse și expertiză comune: Datorită resurselor limitate și complexității securității cibernetice, statele și organizațiile se pot baza pe experiența și resursele comune pentru a dezvolta soluții mai puternice și pentru a se proteja reciproc.

3. Standarde și reguli comune: Cooperarea internațională ajută la stabilirea standardelor și regulilor comune în domeniul securității informațiilor, ceea ce facilitează colaborarea și asigură o abordare mai coezivă a problemelor de securitate cibernetică.

4. Prevenirea conflictelor: Comunicarea și cooperarea în domeniul securității informațiilor pot contribui la evitarea escaladării unor incidente cibernetice și pot reduce riscul de conflicte între state.

5. Protejarea intereselor naționale: Protejarea securității informațiilor este esențială pentru protejarea intereselor naționale, economice și politice ale unei țări, iar cooperarea internațională poate consolida această protecție.

În concluzie, cooperarea internațională în domeniul securității informațiilor este esențială pentru a face față amenințărilor cibernetice într-un mod eficient și pentru a promova securitatea digitală la nivel global.

Existau câteva tendințe semnificative în ceea ce privește creșterea *amenințărilor cibernetice* la nivel Mondial

* Creșterea numărului de atacuri cibernetice: Numărul de atacuri cibernetice, inclusiv atacurile asupra companiilor, organizațiilor guvernamentale și a indivizilor, a continuat să crească semnificativ.
* Ransomware: Atacurile cu ransomware, în care hackerii criptează datele și cer răscumpărare pentru a le restabili, au devenit tot mai frecvente și au afectat o gamă largă de ținte.
* Amenințările la adresa infrastructurii critice: Există o preocupare tot mai mare legată de amenințările cibernetice asupra infrastructurii critice, cum ar fi rețelele electrice și sistemele de apă, care pot avea impacturi grave asupra societății.
* Statele și actorii non-statali: Atacurile cibernetice nu au fost doar operațiuni ale infractorilor cibernetici, ci și ale statelor sau grupurilor non-statale, cum ar fi hackerii sponsorizați de stat sau grupurile de hackeri activiste.
* Creșterea fraudelor online: Fraudele online și escrocheri, cum ar fi phishing-ul și furtul de identitate, au continuat să reprezinte o amenințare semnificativă pentru utilizatorii de internet.

Desigur, securitatea informațiilor este o preocupare majoră în era digitală. Amenințările pot proveni din diverse surse, inclusiv atacuri cibernetice, hărțuire online și furt de identitate. Protejarea datelor devine crucială pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor. O abordare comprehensivă, inclusiv criptarea datelor, actualizarea regulată a software-ului și conștientizarea utilizatorilor, este esențială în fața acestor amenințări în continuă evoluție.

# **Rolul ONU, NATO și alte organizații în promovarea securității informațiilor**

Organizația Națiunilor Unite (ONU), NATO și alte organizații internaționale au un rol crucial în promovarea securității informațiilor într-o lume tot mai interconectată digital. ONU, ca forță globală, își concentrează eforturile pe consolidarea păcii și securității internaționale, inclusiv în domeniul cibernetic. Prin intermediul agențiilor sale specializate, precum Interpol, ONU sprijină statele membre în combaterea amenințărilor cibernetice transfrontaliere.

Există mai multe convenții internaționale și acorduri relevante pentru securitatea informațiilor și cibernetică. Iată câteva exemple notabile:

1. Convenția de la Budapesta asupra criminalității cibernetice (Convenția de la Budapesta): Această convenție, sub auspiciile Consiliului Europei, a fost adoptată în 2001 și a intrat în vigoare în 2004. Ea vizează combaterea criminalității cibernetice prin stabilirea unui cadru legal și cooperarea internațională pentru investigarea și urmărirea penală a infracțiunilor informatice.

2. Convenția privind securitatea informațiilor (Convention on Cybercrime) a Consiliului Europei: Această convenție este legată de Convenția de la Budapesta și a fost concepută pentru a dezvolta un cadru legal mai amplu pentru combaterea infracțiunilor informatice. Ea a fost adoptată în 2004 și a intrat în vigoare în 2004.

3. Acordul de la Paris asupra combaterea terorismului cibernetic: Adoptat în 2018, acest acord reprezintă un efort internațional de a combate utilizarea internetului în scopuri teroriste și de a promova securitatea cibernetică globală.

4. Convenția de la Geneva și Protocoalele Adiționale: Convenția de la Geneva din 1949 și protocoalele sale adiționale stabilesc reguli pentru protejarea persoanelor care nu mai participă la lupte sau sunt afectate de conflicte armate, inclusiv reguli privind securitatea informațiilor și protecția datelor medicale.

5. Tratatul privind nefurnizarea de arme nucleare și reducerea acestora (Tratatul START): Acest tratat între Statele Unite și Rusia include dispoziții privind controlul armelor nucleare și include reglementări pentru securitatea și protecția informațiilor legate de arsenalul nuclear.

Acestea sunt doar câteva exemple de convenții și acorduri internaționale care vizează securitatea informațiilor. Există și alte acorduri bilaterale și multilaterale între state pentru a aborda aspectele legate de securitatea cibernetică și a proteja informațiile sensibile în era digitală.

NATO, alianța militară transatlantică, recunoaște tot mai mult importanța securității cibernetice în cadrul strategiei sale globale. Organizația își propune să dezvolte capacități cibernetice și să întărească cooperarea între statele membre pentru a contracara atacurile cibernetice. Exercițiile comune și schimbul de informații sunt elemente esențiale ale abordării NATO pentru a face față amenințărilor din domeniul cibernetic.

Alte organizații internaționale, cum ar fi Interpol, UNESCO și Consiliul Europei, contribuie, de asemenea, la eforturile globale de securitate cibernetică. Ele facilitează cooperarea între statele membre, promovează standardele și ghidurile pentru securitatea informațiilor și oferă asistență tehnică în dezvoltarea capacităților cibernetice.

Organizațiile precum ONU (Organizația Națiunilor Unite) și NATO (Organizația Tratatului Atlanticului de Nord) au roluri importante în promovarea securității informațiilor la nivel global și regional. Iată câteva aspecte cheie:

- ONU promovează securitatea cibernetică și gestionarea informațiilor prin intermediul diferitelor agenții, cum ar fi ITU (Uniunea Internațională de Telecomunicații) și UNODC (Oficiul Națiunilor Unite pentru Droga și Criminalitate). Ele colaborează pentru dezvoltarea de norme și reguli internaționale pentru utilizarea și protecția spațiului cibernetic.

- ONU facilitează dialogul și cooperarea internațională în ceea ce privește prevenirea conflictelor cibernetice și promovarea utilizării pașnice a tehnologiilor informaționale.

- NATO are o componentă importantă de securitate cibernetică și gestiune a informațiilor. Aceasta include dezvoltarea de politici și strategii pentru protejarea infrastructurii critice, coordonarea răspunsului la incidente cibernetice și îmbunătățirea capabilităților cibernetice ale aliaților.

- NATO promovează schimbul de informații și experiență între statele membre pentru a consolida securitatea cibernetică în întreaga alianță.

Alte organizații regionale și internaționale, cum ar fi UE (Uniunea Europeană), ASEAN (Asociația Națiunilor din Asia de Sud-Est) și altele, au și ele roluri în promovarea securității informațiilor la nivel regional și subregional. Aceste organizații colaborează pentru a dezvolta standarde, acorduri și protocoale de securitate cibernetică, contribuind astfel la protejarea informațiilor și a infrastructurii critice la nivel global și regional.

În ciuda eforturilor acestor organizații, există încă provocări majore în promovarea securității informațiilor la nivel global. Diversitatea de norme și reglementări în domeniul cibernetic, lipsa unei autorități centrale puternice și evoluția rapidă a tehnologiei reprezintă obstacole în calea unei abordări uniforme și eficiente.

În concluzie, ONU, NATO și alte organizații internaționale joacă un rol vital în promovarea securității informațiilor prin intermediul cooperării, schimbului de informații și dezvoltarea capacităților cibernetice. Cu toate acestea, este necesară o abordare continuă și adaptabilă pentru a răspunde la amenințările în continuă evoluție din domeniul cibernetic.

Există mai multe grupuri de lucru internaționale care se concentrează pe securitatea cibernetică și cooperează pentru a aborda diverse aspecte ale acestui domeniu. Iată câteva exemple notabile:

1. Grupul de lucru privind securitatea cibernetică (CSWG) al G7: Grupul de lucru G7 este format din țările membre ale Grupului celor 7 (Canada, Franța, Germania, Italia, Japonia, Marea Britanie și Statele Unite) și se concentrează pe coordonarea politicilor și măsurile de securitate cibernetică la nivel global.

2. Grupul de lucru privind lupta împotriva infracțiunilor informatice al Interpol: Acest grup de lucru se concentrează pe investigarea și combaterea infracțiunilor informatice la nivel internațional și reprezintă o platformă importantă pentru cooperarea între organizațiile de aplicare a legii din diverse țări.

3. Grupul de lucru pentru securitatea cibernetică al APEC (Cooperarea Economică Asia-Pacific): APEC are un grup de lucru dedicat securității cibernetice care se concentrează pe dezvoltarea de politici și practici pentru promovarea securității cibernetice în regiunea Asia-Pacific.

4. Grupul de experți privind protecția infrastructurii critice al Uniunii Europene: Acest grup de experți lucrează la dezvoltarea politicilor și măsurilor pentru protejarea infrastructurii critice în Uniunea Europeană, inclusiv în contextul securității cibernetice.

5. Grupul de lucru privind tehnologia informației și securitatea cibernetică al Organizației pentru Securitate și Cooperare în Europa (OSCE): OSCE are un grup de lucru dedicat securității cibernetice care se concentrează pe gestionarea riscurilor cibernetice și promovarea încrederii și transparenței între statele membre.

Aceste grupuri de lucru internaționale facilitează schimbul de informații, dezvoltarea de politici și măsuri comune și cooperarea între țările și organizațiile implicate în securitatea cibernetică la nivel global și regional.

# **Republica Moldova și cooperare internațională**

Republica Moldova, ca orice altă țară, se confruntă cu numeroase provocări în ceea ce privește securitatea informațiilor și beneficiază de cooperarea internațională pentru a aborda aceste probleme. Câteva aspecte cheie ale cooperării internaționale în domeniul securității informațiilor pentru Republica Moldova includ:

1. *Participarea la organizații internaționale*: Republica Moldova poate coopera cu organizații internaționale, cum ar fi Interpol, Europol și NATO, pentru a accesa resurse și expertiză în domeniul combaterii infracționalității cibernetice și securității informațiilor.

2. *Semnarea acordurilor bilaterale*: Republica Moldova poate încheia acorduri bilaterale de cooperare în domeniul securității informațiilor cu alte state pentru schimbul de informații și resurse în ceea ce privește amenințările cibernetice și infracționalitatea.

3. *Participarea la exerciții și simulări internaționale*: Republica Moldova poate participa la exerciții internaționale de securitate cibernetică și simulări de răspuns la amenințări cibernetice pentru a-și dezvolta capacitățile și a se familiariza cu cele mai bune practici.

4. *Adoptarea standardelor internaționale*: Republica Moldova poate adopta și implementa standarde internaționale pentru securitatea informațiilor, cum ar fi cele din seria ISO/IEC 27000, pentru a se asigura că infrastructura sa cibernetică este robustă și se conformează cerințelor globale.

5. *Crearea unor instituții naționale specializate*: Guvernul Republicii Moldova poate să înființeze instituții specializate și agenții responsabile cu gestionarea securității informațiilor și cu colaborarea cu partenerii internaționali în acest domeniu.

6*. Promovarea educației și conștientizării*: Republica Moldova poate promova educația și conștientizarea în rândul cetățenilor și a sectorului privat în ceea ce privește securitatea informațiilor, pentru a reduce riscurile de atacuri cibernetice și pentru a stimula adoptarea unor practici mai sigure.

7. *Răspuns la incidente cibernetice*: Republica Moldova poate coopera cu alte țări și organizații internaționale pentru a dezvolta capacități de răspuns la incidente cibernetice și pentru a investiga infracțiunile cibernetice.

Cooperarea internațională este esențială pentru Republica Moldova, ca și pentru alte țări, pentru a aborda amenințările cibernetice și pentru a asigura securitatea informațiilor într-un mediu digital tot mai complex și interconectat.

Republica Moldova desfășoară diverse forme de cooperare internațională în domeniul securității informațiilor. Iată câteva exemple:

1. Participarea la exerciții cibernetice internaționale: Republica Moldova poate participa la exerciții și simulări internaționale în domeniul securității cibernetice, organizate de organizații precum NATO sau Europol. Aceste exerciții permit țării să își testeze capacitățile de răspuns la amenințări cibernetice și să colaboreze cu parteneri internaționali pentru îmbunătățirea securității informațiilor.

2. Schimbul de informații cu organizații de securitate internațională: Republica Moldova poate coopera cu organizații internaționale precum Interpol și Europol pentru schimbul de informații legate de infracțiunile cibernetice și a altor amenințări la adresa securității informațiilor.

3. Participarea la conferințe și forumuri internaționale: Guvernul și instituțiile din Republica Moldova pot participa la conferințe, forumuri și evenimente internaționale legate de securitatea cibernetică, pentru a-și împărtăși experiența și pentru a învăța de la alți experți din întreaga lume.

4. Colaborarea cu organizații non-guvernamentale și sectorul privat: Republica Moldova poate colabora cu organizații non-guvernamentale și companii private pentru a dezvolta proiecte și inițiative în domeniul securității informațiilor. Aceasta include eforturile de conștientizare, educație și promovarea unor practici mai sigure în utilizarea tehnologiei.

5. Implementarea standardelor internaționale: Republica Moldova poate adopta și implementa standardele internaționale în domeniul securității informațiilor, cum ar fi cele din seria ISO/IEC 27000, pentru a asigura conformitatea cu cerințele globale și pentru a stabili baze solide pentru protecția datelor.

Aceste exemple ilustrează modul în care Republica Moldova poate colabora cu parteneri internaționali pentru a promova securitatea informațiilor și pentru a aborda amenințările cibernetice într-un mediu global tot mai complex. Prin cooperarea internațională, țara poate beneficia de expertiză și resurse suplimentare pentru a-și întări capacitățile în domeniul securității cibernetice.

# **Concluzii și recomandări**

Securitatea informațiilor a devenit o problemă vitală în era digitală, deoarece informațiile și tehnologiile digitale joacă un rol crucial în societatea contemporană. În acest context, cooperarea internațională în domeniul securității informațiilor este esențială pentru protejarea intereselor naționale și internaționale. Acest eseu explorează cadrul de cooperare pe arena internațională în domeniul securității informațiilor și analizează rolul organizațiilor internaționale în promovarea acestei cooperări.

Cooperarea internațională în securitatea informațiilor este esențială din mai multe motive. În primul rând, amenințările cibernetice nu cunosc granițe naționale. Atacurile cibernetice pot fi lansate de oriunde din lume și pot afecta ținte din diferite țări. Prin urmare, este crucial să existe un cadru de cooperare care să permită schimbul de informații și coordonarea acțiunilor pentru contracararea acestor amenințări.

Organizațiile internaționale joacă un rol semnificativ în promovarea cooperării în domeniul securității informațiilor. Una dintre cele mai importante organizații este Organizația Națiunilor Unite (ONU). ONU a recunoscut importanța securității cibernetice prin elaborarea unor directive și rezoluții care invită statele membre să coopereze pentru a combate amenințările cibernetice. De asemenea, ONU găzduiește Grupul de Experți al ONU pentru Securitatea Cibernetică, care reunește statele membre pentru a dezvolta măsuri de securitate cibernetică.

În plus, există organizații regionale și acorduri bilaterale care promovează cooperarea în domeniul securității informațiilor. De exemplu, Uniunea Europeană are o Agendă Digitală care include măsuri pentru consolidarea securității cibernetice. Statele membre ale UE cooperează pentru a dezvolta standarde comune și pentru a se ajuta reciproc în caz de atacuri cibernetice.

Cu toate acestea, există încă provocări majore în ceea ce privește cooperarea internațională în securitatea informațiilor. Una dintre acestea este dificultatea de a ajunge la un consens privind normele și regulile în domeniul cibernetic. Statele au interese și perspective diferite, ceea ce face dificilă stabilirea unui cadru comun de acțiune. De asemenea, problema confidențialității și a protecției datelor personale rămâne o preocupare majoră în cooperarea internațională în securitatea informațiilor.

În concluzie, cooperarea internațională în domeniul securității informațiilor este esențială în lumea digitală contemporană. Organizațiile internaționale, cum ar fi ONU și NATO, joacă un rol crucial în promovarea acestei cooperări, dar există încă provocări de depășit. Cu toate acestea, eforturile continue pentru dezvoltarea unui cadru comun și pentru abordarea amenințărilor cibernetice într-un mod coordonat sunt esențiale pentru asigurarea securității informațiilor la nivel global.m

Viitorul Cooperării Internaționale în Securitatea Informațională este complex și impune adaptarea continuă la evoluțiile tehnologice și amenințările cibernetice. Unele aspecte cheie includ:

* Dezvoltarea Tehnologică Accelerată:

- Integrarea tehnologiilor emergente precum inteligența artificială și computația cuantică.

- Necesitatea standardizării și colaborării pentru a gestiona riscurile asociate cu inovațiile tehnologice.

* Consolidarea Legislației și Normelor Internaționale:

- Adoptarea unor standarde comune pentru securitatea informațională la nivel global.

- Crearea și consolidarea tratatelor internaționale privind răspunsul la amenințări cibernetice.

* Intensificarea Cooperării Public-Privat:

- Creșterea colaborării între guverne și sectorul privat pentru a îmbunătăți protecția împotriva atacurilor cibernetice.

- Implementarea partajării de informații între organizațiile private și autoritățile guvernamentale.

* Focus pe Educație și Dezvoltare de Competențe:

- Investiții în programe de educație și formare în domeniul securității cibernetice la nivel global.

- Dezvoltarea și consolidarea forței de muncă specializate în securitatea informațională.

* Abordarea Amenințărilor Hibrice:

- Integrarea eforturilor în gestionarea amenințărilor cibernetice în contextul amenințărilor hibrice.

- Cooperarea strânsă pentru prevenirea și gestionarea atacurilor care combină elemente cibernetice, informaționale și clasice.

* Adaptarea la Schimbările Geopolitice:

- Acomodarea la schimbările în peisajul geopolitic și ajustarea cooperării în funcție de acestea.

- Gestionarea tensiunilor și construirea de parteneriate solide în ciuda diferențelor politice.

Aceste direcții pot contribui la o cooperare internațională eficientă în securitatea informațională și la gestionarea provocărilor viitoare.

# **Bibliografie**

1. A History of Cyberspace. Per Concordiam, v. 7, nr. 2, 2016, p. 64-65.
2. Busuncian T. Securitatea informațională și activitatea serviciilor de informații în contextul globalizării. Studii naționale de securitate. Revistă științifico-practică Nr. 1 (1) 2020. ISSN 2587-3822 CZU 004.056: 355.40 DOI: 10.5281/zenodo.3989164. Chișinău, 2020, p. 66-78.
3. Busuncian T. Parametrii instituționali ai securităţii informaționale. Materialele conferinței ştiinţifico-practice naționale „Mandatul de securitate: probleme actuale de interpretare, legislație şi practică”. Serviciul de Informaţii şi Securitate al Republicii Moldova Institutul Naţional de Informaţii şi Securitate „Bogdan, Întemeietorul Moldovei”. Chișinău, 2020, p. 71-75.
4. Busuncian T. Colaborarea internațională a serviciilor speciale în combaterea terorismului. Teză de doctor în politologie. Chișinău, 2013, 182 p.
5. Hotărârea Guvernului Nr. 746 din 18.08.2010 "Cu privire la aprobarea Planului Individual de Acţiuni al Parteneriatului Republica Moldova – NATO actualizat" Monitorul Oficial al Republicii Moldova No. 166-168 din 14.09.2010.
6. 1.Maior G. C., Intelligence. În: Intelligence, 2008, anul V, serie nouă, nr. 11, p. 1-13.
7. 2. Faligot R., Kauffer R. Istoria mondială a serviciilor secrete. Bucureşti: Nemira, 2002, vol. 3, 4, 532 p.
8. 3. Forcade O. , Laurent S. Serviciile Secrete. Puterea şi informaţia secretă în lumea modernă. Bucureşti: Cartier, 2008, 280 p.
9. 4. Tsang S., Serviciile de informaţii şi drepturile omului în era terorismului global. Bucureşti: Univers Enciclopedic, 2008. 259 p.
10. 5. Cтаркин С. В., Аналитические институты разведывательного сообщества США во внешнеполитическом процессе. Нижний Новгород: Стимул- CT, 2011, 466 с. 6. Устинов В. В. Международно-правовые проблемы борьбы с терроризмом. Москва, 2002, 594 с.