



## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ, ПОИСК И ВОССТАНОВЛЕНИЕ

**Иминов Аблурасул Абдулатипович**

Начальник кафедры Цифровых технологий и  
информационной безопасности Академии МВД  
Республики Узбекистан Ташкент, 100197, Узбекистан

e-mail: [fargan77@bk.ru](mailto:fargan77@bk.ru)

[orcid.org/0009-0005-2423-050X](https://orcid.org/0009-0005-2423-050X)

**Курбанова Гавхарой Собировна**

курсант 3-го учебного курса, обучающаяся по  
специальности "Профилактика правонарушений"  
Академии МВД Республики Узбекистан

***Аннотация:** В данной статье рассматриваются вопросы обеспечения информационной безопасности в киберпространстве, а также процессы поиска, выявления и восстановления после киберинцидентов. Раскрываются основные принципы защиты информации — конфиденциальность, целостность и доступность, анализируются современные киберугрозы и методы их обнаружения. Особое внимание уделяется системам мониторинга, аудиту безопасности, резервному копированию данных и разработке планов реагирования на инциденты. Подчеркивается важность комплексного подхода, включающего технические, организационные и правовые меры, а также роль международного сотрудничества в борьбе с киберпреступностью.*

***Ключевые слова** информационная безопасность, киберпространство, киберугрозы, защита информации, конфиденциальность, целостность, доступность, кибератака, вредоносное программное обеспечение, фишинг, DDoS-атаки, обнаружение угроз, резервное копирование, восстановление данных, киберпреступность.*

***Abstract:** This article examines the issues of ensuring information security in cyberspace, as well as the processes of searching, detecting, and recovering after cyber incidents. The main principles of information protection - confidentiality,*

*integrity, and accessibility - are revealed, and modern cyber threats and their detection methods are analyzed. Special attention is paid to monitoring systems, security audits, data backup, and incident response plans. The importance of a comprehensive approach, including technical, organizational, and legal measures, as well as the role of international cooperation in combating cybercrime, is emphasized.*

**Keywords:** *information security, cyberspace, cyber threats, information protection, privacy, integrity, accessibility, cyberattack, malicious software, phishing, DDoS attacks, threat detection, backup, data recovery, cybercrime.*

В условиях стремительного развития цифровых технологий и глобальной информатизации общества киберпространство стало неотъемлемой частью повседневной жизни человека, бизнеса и государства. Электронная коммерция, онлайн-банкинг, государственные цифровые сервисы, облачные технологии и социальные сети значительно упростили процессы обмена информацией.

Однако вместе с преимуществами цифровой эпохи возникли и новые риски — киберугрозы, направленные на кражу данных, нарушение работы информационных систем и нанесение финансового или репутационного ущерба.

Обеспечение информационной безопасности в киберпространстве является одной из приоритетных задач современного общества. Особое значение приобретают процессы своевременного обнаружения угроз, их поиска и эффективного восстановления данных после инцидентов.

Теоретической основой исследования послужили нормативно-правовые документы в сфере информационной безопасности, научные труды отечественных и зарубежных авторов, а также международные стандарты управления информационной безопасностью.

**Методология исследования включает:**

- анализ научной литературы и нормативных источников;
- сравнительный анализ современных киберугроз;
- системный подход к обеспечению защиты информации;
- обобщение практических методов поиска и восстановления после киберинцидентов.

Информационная безопасность определяется как состояние защищенности информации и информационных систем от несанкционированного доступа, изменения, разрушения или распространения. В киберпространстве она основывается на трех ключевых принципах:

1. **Конфиденциальность** — защита информации от несанкционированного доступа.
2. **Целостность** — сохранение точности и неизменности данных.
3. **Доступность** — обеспечение доступа к информации для авторизованных пользователей.

Анализ показал, что современное киберпространство характеризуется разнообразием угроз, среди которых наиболее распространены:

- вредоносное программное обеспечение (вирусы, трояны, программы-вымогатели);
- фишинг и методы социальной инженерии;
- DDoS-атаки;
- несанкционированный доступ и взломы;
- внутренние угрозы со стороны сотрудников.

Для поиска и выявления киберугроз применяются:

1. Системы обнаружения и предотвращения вторжений (IDS/IPS).
2. Антивирусное программное обеспечение.
3. Мониторинг журналов событий (логов).

4. Аудит безопасности.
5. Пентестинг (тестирование на проникновение).

Установлено, что наиболее эффективной является многоуровневая система защиты, сочетающая технические средства и организационные меры.

Несмотря на развитие технологий защиты, полностью исключить вероятность кибератак невозможно. Поэтому важнейшим элементом системы информационной безопасности является механизм восстановления после инцидентов.

Основные меры восстановления включают:

- регулярное резервное копирование данных (backup);
- разработку и внедрение плана реагирования на инциденты;
- использование систем аварийного восстановления (Disaster Recovery);
- анализ причин инцидентов и устранение выявленных уязвимостей.

Кроме того, существенную роль играет государственная политика в сфере кибербезопасности, разработка нормативно-правовой базы и международное сотрудничество, поскольку кибератаки носят трансграничный характер.

Обеспечение информационной безопасности в киберпространстве является сложной и многогранной задачей, требующей комплексного подхода. Эффективная защита возможна только при сочетании современных технических средств, грамотной организации процессов, регулярного мониторинга и подготовки квалифицированных специалистов.

Своевременный поиск и выявление угроз позволяют минимизировать ущерб, а грамотно организованная система восстановления обеспечивает устойчивость информационных систем к киберинцидентам.

В условиях цифровой трансформации общества совершенствование механизмов кибербезопасности становится необходимым условием стабильности и безопасного развития современного мира.

### **СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. Доктрина информационной безопасности Российской Федерации. — М., 2016.
2. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ.
3. Касперский Е. В. Компьютерные вирусы в MS-DOS. — М.: Мир, 1992.
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. — М.: ФОРУМ, 2020.
5. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: Горячая линия – Телеком, 2018.
6. ISO/IEC 27001:2022. Information security management systems — Requirements.
7. Stallings W. Network Security Essentials: Applications and Standards. — Pearson, 2018.
8. Whitman M., Mattord H. Principles of Information Security. — Cengage Learning, 2021.
9. Takhirzhanovich G. F. et al. IMPROVEMENT OF THE ACTIVITIES OF PREVENTION INSPECTORS IN THE PREVENTION OF RECIDIVIST CRIMES AMONG WOMEN //Shokh Articles Library. – 2026. – Т. 1. – №. 1.
10. Takhirzhanovich G. F. et al. IMPROVEMENT OF MATERIAL AND TECHNICAL SUPPORT FOR THE ACTIVITIES OF THE CRIME PREVENTION SERVICE OF INTERNAL AFFAIRS BODIES //Shokh Articles Library. – 2026. – Т. 1. – №. 1.

11. Ustayevich K. A. et al. IMPROVEMENT OF THE ORGANIZATION AND COORDINATION OF THE ACTIVITIES OF SUPPORT POINTS OF INTERNAL AFFAIRS BODIES //Shokh Articles Library. – 2026. – T. 1. – №. 1.
12. Eshqobilov A., Farrux G. A. PROFILAKTIKA INSPEKTORLARINING KIBERJINOYATCHILIKNI OLDINI OLIISH FAOLIYATI //Central Asian Journal of Multidisciplinary Research and Management Studies. – 2025. – T. 2. – №. 6. – C. 216-220.
13. Qizi I. M. N., Taxirjanovich G. A. F. PROFILAKTIKA INSPEKTORINING HUQUQBUZALIKLAR PROFILAKTIKASIDA ADLIYA ORGANLARI BILAN HAMKORLIGI //Central Asian Journal of Multidisciplinary Research and Management Studies. – 2025. – T. 2. – №. 1. – C. 34-38.
14. Qizi M. M. M., Taxirjanovich G. A. F. YOSHLAR BILAN ISHLASHDA JINOYATCHILIKKA QARSHI KURASHISH MAVZUSIDA //Central Asian Journal of Multidisciplinary Research and Management Studies. – 2025. – T. 2. – №. 1. – C. 44-47.
15. Takhirzhanovich G. F. et al. IMPROVEMENT OF THE ACTIVITIES OF PREVENTION INSPECTORS IN THE PREVENTION OF RECIDIVIST CRIMES AMONG WOMEN //Shokh Articles Library. – 2026. – T. 1. – №. 1.
16. Ustayevich K. A. et al. IMPROVEMENT OF THE ORGANIZATION AND COORDINATION OF THE ACTIVITIES OF SUPPORT POINTS OF INTERNAL AFFAIRS BODIES //Shokh Articles Library. – 2026. – T. 1. – №. 1.
17. Toshboyev F. E. et al. QADIMGI MIGRATSIYALARNING USTURUSHONA IJTIMOIIY IQTISODIY HAYOTIGA TA’SIRI //ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ. – 2026. – Т. 85. – №. 1. – С. 130-138.
18. Sevinsh S. MIGRATSIYA VA QOCHOQLAR MUAMMOSI //Ta'lim innovatsiyasi va integratsiyasi. – 2025. – Т. 57. – №. 1. – С. 265-268.

- 19.Qizi I. M. N., Taxirjanovich G. A. F. PROFILAKTIKA INSPEKTORINING HUQUQBUZALIKLAR PROFILAKTIKASIDA ADLIYA ORGANLARI BILAN HAMKORLIGI //Central Asian Journal of Multidisciplinary Research and Management Studies. – 2025. – T. 2. – №. 1. – C. 34-38.
- 20.Eshqobilov A., Farrux G. A. PROFILAKTIKA INSPEKTORLARINING KIBERJINOYATCHILIKNI OLDINI OLISH FAOLIYATI //Central Asian Journal of Multidisciplinary Research and Management Studies. – 2025. – T. 2. – №. 6. – C. 216-220.
- 21.Eshqobilov A., Farrux G. A. PROFILAKTIKA INSPEKTORLARINING KIBERJINOYATCHILIKNI OLDINI OLISH FAOLIYATI //Central Asian Journal of Multidisciplinary Research and Management Studies. – 2025. – T. 2. – №. 6. – C. 216-220.
- 22.Qizi I. M. N., Taxirjanovich G. A. F. PROFILAKTIKA INSPEKTORINING HUQUQBUZALIKLAR PROFILAKTIKASIDA ADLIYA ORGANLARI BILAN HAMKORLIGI //Central Asian Journal of Multidisciplinary Research and Management Studies. – 2025. – T. 2. – №. 1. – C. 34-38.