基于信息化下的机要保密工作探析

安娜
（包头钢铁＜集团＞铁捷物流有限公司，内蒙古自治区　包头　014060）

【摘　要】随着信息技术的快速发展和广泛应用，机要保密工作面临着前所未有的挑战。本文旨在探讨信息化背景下机要保密工作的新特点、新问题，并提出相应的对策和建议，以期提升机要保密工作的整体效能。

【关键词】信息化；机要保密；工作探析

在当今信息化时代，信息技术的迅猛发展给各行各业带来了翻天覆地的变化，同时也对机要保密工作提出了更高的要求。传统的机要保密方式已难以满足新形势下的需求，因此，如何适应信息化发展的要求，加强机要保密工作，成为当前亟待解决的问题。.

一、信息化下机要保密工作的新特点

（一）信息量大增

随着大数据、云计算等先进技术的深入应用，机要保密工作面临着前所未有的挑战。这些技术不仅极大地促进了信息的生成和流动，还使得机要保密工作中需要处理的信息量呈现出爆炸性增长的趋势。这种增长不仅仅是数量上的，更是复杂性和多样性上的。机要保密人员现在需要处理的信息类型更加多样，包括结构化数据、半结构化数据和非结构化数据等，每种数据都有其独特的处理要求和风险点。

此外，大数据和云计算技术还带来了信息处理和存储方式的变革。传统的信息处理方式已经难以应对如此庞大的信息量，而云计算等新技术则为高效处理这些信息提供了可能。然而，这也对机要保密工作提出了更高的要求，如何在这些新技术环境下确保信息的安全、完整和可用，成为了机要保密人员必须面对和解决的问题。因此，机要保密工作必须紧跟时代步伐，加强技术研发和应用，提升信息处理能力和安全防护水平，以应对大数据、云计算等技术带来的挑战。

（二）传输速度快

信息技术的快速发展，特别是网络通信技术的革新，使得信息的传输速度得到了空前的提升。无论是文字、图片还是视频，都能在短时间内实现跨地域的快速传输。这种传输速度的提升，为各行各业带来了极大的便利，但同时也给机要保密工作带来了更加严峻的时间压力。在机要保密领域，信息的传输速度直接关系到机密信息的暴露风险。传输速度越快，信息在传输过程中被截获或窃取的可能性就越大。快速的信息传输也意味着机要保密人员需要在更短的时间内对信息进行处理、存储和销毁，以防止信息泄露或被非法利用。

所以，机要保密工作必须适应信息技术快速发展的趋势，加强技术研发和应用，提升信息处理效率和安全防护能力。并加强人员培训和管理，提高人员的反应速度和应对能力，确保在有限的时间内能够有效地完成机要保密任务，保障机密信息的安全与完整。只有这样，才能在信息技术的快速发展中立于不败之地，为国家的安全和利益提供坚实的保障。

（三）环境复杂多变

信息技术的普及和深入应用，无疑为现代社会带来了便捷与高效，但同时也使得机要保密工作的环境变得前所未有的复杂多变。这其中，网络攻击和病毒入侵等新型威胁的不断涌现，成为了机要保密领域面临的严峻挑战。网络攻击者利用先进的技术手段，不断寻找和利用系统的漏洞，企图窃取或破坏机密信息。而病毒和恶意软件的传播，更是防不胜防，它们隐藏在看似正常的文件和程序中，一旦触发，就可能对机密信息系统造成严重的破坏。

这些新型威胁的出现，不仅要求机要保密人员具备更高的技术水平和更快的反应速度，还要求他们不断更新和完善安全防护策略，以应对日益复杂多变的网络环境。所以，机要保密工作必须时刻保持警惕，加强技术研发和投入，提升人员的专业素质和综合能力，确保在信息技术普及的大背景下，能够有效地应对各种新型威胁，保障机密信息的安全与完整。

二、信息化对机要保密工作的影响

（一）信息传输方式的变革

传统的纸质文件传输方式，曾以其稳定可靠的特性在长时间内占据主导地位。然而，随着信息技术的迅猛发展，电子文档逐渐崭露头角，成为信息传输的新宠。电子文档以其高效便捷的特点，极大地提升了信息传输的速度，使得工作人员可以在短时间内轻松分享和获取大量信息。与纸质文件相比，电子文档在传输过程中更容易受到黑客攻击和病毒感染，从而导致信息泄露的风险大大增加。

（二）信息存储方式的改变

云存储与大数据技术的兴起，无疑为现代社会的信息存储带来了革命性的变革。使得用户可以轻松地将海量数据上传至云端，随时随地访问和共享，极大地提高了信息存储的便捷性。不仅如此，这些技术还为企业和组织提供了强大的数据分析工具，帮助他们从海量数据中挖掘出有价值的信息。然而，这些技术的广泛应用也带来了安全隐患。由于数据在云端集中存储，一旦云服务提供商的安全措施不到位或遭受黑客攻击，用户的数据就可能面临被窃取或篡改的风险。

（三）信息处理方式的升级

人工智能与机器学习等尖端技术的广泛应用，为信息处理领域注入了新的活力。这些技术使得计算机能够自主学习、不断优化，并在处理海量信息时展现出惊人的效率。无论是自动化的数据分类、智能推荐，还是复杂的数据分析任务，人工智能与机器学习都展现出了强大的实力。然而，技术的双刃剑效应再次显现。随着这些技术的普及，新的安全隐患也逐渐浮出水面。例如，恶意软件可能会利用机器学习技术来躲避安全软件的检测，或者通过模仿用户行为来实施网络钓鱼攻击。因此，在欣赏人工智能与机器学习带来的便利与高效的同时，必须高度警惕这些新兴技术可能被滥用的风险。信息安全界需要与时俱进，深入研究新技术带来的新挑战，并发展出相应的防御策略，以确保技术的健康发展与社会的安全稳定。

三、信息化下机要保密工作面临的新问题

（一）技术防范难度加大

随着黑客技术的持续进步和演变，网络攻击手段已经变得日益复杂和难以预测。这些黑客不仅具备高超的编程技能，还深谙网络安全漏洞，能够针对各种系统发动精准的攻击。他们所使用的工具和方法也在不断更新，从简单的病毒、木马到复杂的钓鱼攻击、零日漏洞利用，每一次攻击都可能给机要保密系统带来严重的威胁。

（二）人员管理难度增加

在信息化的大背景下，随着科技的迅速发展和全球化的推进，人员的流动性日益增强。这种流动性不仅体现在地理位置的变迁，也涉及到行业、职位以及工作内容的频繁变化。这种高度的流动性对组织的安全管理提出了新的挑战。

（三）法律制度滞后

随着信息技术的迅猛发展，新的技术、新的应用层出不穷，它们在为我们的生活和工作带来便利的同时，也给现有的法律法规体系带来了挑战。现有法律法规在信息化方面的规定往往相对滞后，难以及时跟上新技术的发展步伐。这导致在实际应用中，一些新技术、新应用可能处于法律的灰色地带，既无法得到有效规范，也给不法分子留下了可乘之机。

（四）保密管理制度不健全

部分单位在机要保密管理方面存在明显的不足，其核心问题在于管理制度的不完善。这些单位往往缺乏一套系统、全面且适应性强的机要保密管理制度，导致在日常工作中无法对涉密信息进行有效的管理和控制。更为严重的是，由于缺乏有效的监督和约束机制，这些管理上的漏洞可能长期存在而得不到及时的纠正和处理，从而极大地增加了机密信息泄露的风险。因此，完善机要保密管理制度，加强监督和约束，是这些单位亟待解决的重要问题。

四、加强信息化下机要保密工作的对策和建议

（一）加强技术防范（物理隔离）

为了有效应对信息化时代带来的安全挑战，机要保密系统必须采用先进的加密技术和防火墙技术等手段，以提升其安全防护能力。这些技术手段能够确保机要信息在传输和存储过程中的安全保密性，防止未经授权的访问和泄露。具体而言，加密技术通过对敏感信息进行编码，使得只有拥有相应密钥的授权用户才能解密并访问原始数据。这种技术能够有效地保护机要信息不被窃取或篡改。而防火墙技术则能够在网络边界处对进出的数据进行实时监控和过滤，阻止恶意攻击和非法访问，确保机要保密系统的网络安全。通过采用这些先进的技术手段，机要保密系统可以构筑起坚实的安全防线，最大程度地保护机要信息的安全性和完整性，为国家和组织的机密保密工作提供有力保障。

（二）强化人员管理

为了确保机要保密工作的万无一失，建立严格的人员准入机制至关重要。这一机制应涵盖详尽的背景调查、严格的资格审查以及必要的安全测试，确保每一位涉密人员都具备高度的可靠性和忠诚度。同时，加强对涉密人员的安全教育和培训也不容忽视。通过定期的安全培训课程，强化人员的安全意识，使他们时刻保持警惕，防范潜在的安全风险。不断提高人员的技能水平，为保障机要保密工作的提供条件。随着技术的不断发展，涉密人员需要不断更新自己的知识储备，掌握最新的安全技术和工具。通过组织技术交流会、提供专业培训资源等方式，可以帮助涉密人员不断提升自身的技能水平，更好地应对日益复杂的安全挑战。

（三）完善法律法规

为了应对信息化时代对机要保密工作提出的新挑战，加快制定和完善与信息化相关的法律法规显得

尤为迫切。这些法律法规应明确界定信息化技术在机要保密领域的应用范围、操作规范和责任主体，确保各项工作有法可依、有章可循。同时，法律法规还应强化对违法行为的惩处力度，提高法律的威慑力，从根本上杜绝信息泄露和网络安全事件的发生。通过构建完善的法律体系，可以为机要保密工作提供坚实的法律后盾，确保机要信息的安全和保密不受侵害。此外，随着技术的不断进步和威胁的不断演变，相关法律法规也需要保持动态更新，及时适应新形势、新需求，为机要保密工作提供持续、有效的法律保障。

（四）建立应急响应机制

针对信息化时代可能出现的各种安全事件，如数据泄露、网络攻击、系统瘫痪等。为此，必须建立一套快速、高效的应急响应机制，以便在第一时间做出反应，最大程度地减少损失。这一应急响应机制应包括以下几个方面：首先，要建立专门的应急响应团队，由具备丰富经验和专业技能的人员组成，负责处理各种安全事件。其次，要制定详细的应急响应计划，明确各种安全事件的处理流程、责任分工和协作方式。这样，在事件发生时，相关人员能够迅速按照计划行动，避免混乱和延误。此外，应急响应机制还应包括预警和监测环节。通过部署先进的安全监测工具和系统，实时监测网络流量、系统日志等关键信息，及时发现异常和潜在威胁。一旦发现可疑活动或攻击行为，应立即启动应急响应程序，进行处置和防范。

在应急响应过程中，需要加强信息沟通和协作工作。要保持与相关部门和机构的紧密联系，及时共享信息、协调行动，形成合力应对安全事件。同时，还要及时向上级主管部门报告事件进展和处理情况，接受指导和支持。总之，建立快速、高效的应急响应机制是保障信息化安全的重要手段。通过这一机制，我们能够迅速应对各种安全事件，最大程度地减少损失和风险，确保机要保密工作的顺利进行。

（五）深化跨部门协作

在信息化时代背景下，机要保密工作面临着前所未有的挑战和威胁。为了有效应对这些挑战，加强机要保密工作与其他部门的沟通与协作显得尤为重要。首先，机要保密工作不是孤立的，它与众多部门都有着千丝万缕的联系。例如，信息技术部门负责信息系统的建设和维护，而机要保密部门则负责确保这些系统中的信息安全。如果两者之间缺乏有效的沟通和协作，就可能导致信息系统的安全漏洞无法及时被发现和修复，从而给机密信息的安全带来严重威胁。进一步加强机要保密工作与信息技术部门的沟通与协作至关重要。其次，除了信息技术部门外，机要保密工作还需要与人力资源、行政管理、法务等多个部门进行紧密配合。人力资源部门负责人员的招聘、培训和管理，而机要保密部门则需要对这些人员进行严格的保密审查和教育。行政管理部门负责单位的日常管理和运作，而机要保密部门则需要在这些管理和运作中嵌入保密要求和措施。法务部门负责法律事务的处理和咨询，而机要保密部门则需要与法务部门共同研究和应对涉及机密信息的法律问题。通过加强机要保密工作与这些部门的沟通与协作，对于确保机密信息的安全至关重要。最后，加强沟通与协作还需要建立有效的机制和平台。一方面，可以建立定期的沟通会议制度，让各部门了解机要保密工作的最新动态和需求，同时也让机要保密部门了解其他部门的工作进展和困难。另一方面，可以建立信息共享平台，让各部门能够及时获取和分享与机要保密相关的信息和资源。通过这些机制和平台的建设，可以进一步加强机要保密工作与其他部门的沟通与协作，形成合力共同应对信息安全威胁。

五、结语

总之，信息化的发展给机要保密工作带来了新的挑战和机遇。只有不断适应新形势、新要求，加强技术创新和管理创新，才能确保机要保密工作的安全稳定。随着信息技术的不断进步和应用领域的不断拓展，机要保密工作将面临更加复杂多变的局面，需要我们保持高度的警惕和敏锐的洞察力，以应对各种挑战和风险。

参考文献：

[1] 叶群慧，陈晓燕 . 办公信息化背景下保密工作研究 [J]. 管理学家 ,2019(8):62-63.

[2] 于家德 . 信息化条件下机要安全保密工作探析 [J]. 中国新通信 ,2021(5):139-140.

[3] 唐松，张一帆，谢若龑 . 智能互联时代信息化保密安全工作问题与对策 [J]. 办公室业务 ,2021(14):117,149.

[4] 闫静 . 基于业务工作与保密工作融合的保密一体化管理体系构建 [J]. 中国管理信息化 ,2022(3):112-114.

[5] 赵晓棠 . 信息化背景下单位保密管理工作创新思考 [J]. 科学与信息化 ,2021(31):190-193.

[6] 崔嘉琪 , 白雨 . 信息化视角下企业保密管理工作有效性创新 [J]. 现代企业 ,2022(6):13-14.

[7] 张玲宁 . 网络信息化时代保密管理问题研究 [J]. 网络安全和信息化 ,2021(1):17-19.

[8] 秦玲 , 张军 , 熊学仕 , 等 . 从“保密信息化”到“信息化保密”的距离 [J]. 保密科学技术 ,2019(10):63-65.