信息安全技术在保护知识产权中的应用

姜靖
西藏熙安信息技术有限责任公司　西藏自治区拉萨　850000

【摘　要】信息化日益发展的时代背景下，知识产权的重要性愈发凸显。企业机密、技术创新及个人创意等无形资产，均急需得到周密的保护，以防范潜在的侵权风险。信息安全技术，通过其先进的加密、访问控制及入侵检测手段，为知识产权筑起了一道坚固的保护墙。然而，网络攻击的不断演变和法律规制的不足，仍为知识产权保护带来了严峻挑战。本文旨在深入探讨信息安全技术在保护知识产权中的实际应用与价值，分析当前面临的问题，并提出有效的应对策略，以期为相关研究与实践提供有益的借鉴。

【关键词】信息安全；技术保护；知识产权

Application of information security technology in intellectual property protection

Jiang Jing
Xizang Xinan Information Technology Co.，LTD Lhasa City，Tibet Autonomous Region　850000

【Abstract】Under the background of information development，the importance of intellectual property is becoming more and more prominent. Intangible assets such as enterprise secrets，technological innovation and personal creativity are all in urgent need of careful protection to prevent potential infringement risks. Information security technology，through its advanced encryption，access control and intrusion detection means，has built a strong protective wall for intellectual property rights. However，the continuous evolution of cyber attacks and the lack of legal regulations still bring severe challenges to intellectual property protection. This paper aims to explore the practical application and value of information security technology in the protection of intellectual property rights，analyze the current problems，and put forward effective coping strategies，in order to provide useful reference for relevant research and practice.

【Key words】information security；technology protection；intellectual property rights

引言

信息安全技术在知识产权保护中扮演着至关重要的角色。该技术利用尖端的加密技术和严格的访问控制机制，确保知识产权的安全与完整，有效防止非法访问和数据篡改。同时，信息安全技术还助力数字版权的精细化管理与追踪，推动创新成果的正版传播，进一步挖掘知识产权的商业价值。对于企业而言，这些技术不仅是保护核心资源和创新产出的关键，更能显著提升其市场竞争优势。因此，深入研究信息安全技术在知识产权保护中的应用，对于增强企业核心竞争力、推动科技创新和经济增长具有重要意义。

一、信息安全技术在保护知识产权中的重大价值

（一）确保知识产权的严密保护

信息安全技术为知识产权提供坚不可摧的保障。加密技术，如 AES 和 RSA 算法，为知识产权数据构筑了强大的安全屏障，防止数据在传输和存储中被窃取或篡改。同时，访问控制技术通过严格的身份和权限管理，如基于角色和属性的访问控制，确保了知识产权数据仅对授权人员开放。此外，入侵检测与防御系统实时监控网络异常，有效抵御网络威胁，而数据备份与恢复技术则确保了知识产权数据的安全性和完整性。

（二）助力创新成果的合法利用

信息安全技术推动创新成果的规范使用。数字版权管理（DRM）技术实现对知识产权的精细控制，防止未经授权的使用。数字水印技术为追踪和验证知识产权来源提供有效手段。新兴的区块链技术则通过去中心化记录和智能合约，增强知识产权管理的透明度和可信度，保障交易安全可追溯。这些技术共同为创新成果的合法利用提供坚实支撑。

（三）提升企业核心竞争力

信息安全技术是企业保护核心竞争力的关键。通过加密、访问控制和入侵检测等多重措施，企业能有效防止信息泄露和被盗取，保护创新产出和商业秘密。同时，这些技术还提升企业知识产权管控效率，确保创新成果的合法授权和规范使用，进而增强知识产权的市场价值。此外，信息安全技术还助力企业构建完善的风险防控体系，为稳健发展提供保障，并为企业探索新商业模式和市场机遇创造可能。

二、信息安全技术在知识产权保护应用中所面临的挑战

（一）技术防御措施尚不完善

尽管信息安全技术在知识产权保护方面已取得显著进展，但仍然存在技术防御不够全面的问题。随着科技日新月异，信息安全技术必须持续更新，以对抗不断演变的安全威胁。然而，当前技术更新的步伐常常滞后于黑客攻击手段的创新，使得众多企业和组织在保护知识产权时感到力不从心。黑客及恶意行为者持续开发出新型攻击手段，诸如零日漏洞利用、社会工程学攻击等，令传统防御机制难以应对。同时，虽然加密技术在保护知识产权方面发挥了一定作用，但随着计算能力的增强，多种加密算法正面临被破解的威胁。特别是在量子计算技术逐步走向实用化的背景下，现有的加密体系可能将不再安全可靠。此外，现有的信息安全技术主要聚焦于网络层面的防护，却往往忽视了物理安全的重要性。例如，物理访问控制不严格可能导致硬件设备失窃或数据被直接窃取，对知识产权构成严重威胁。另一方面，信息安全技术在不同行业的应用成效存在差异。在医疗、金融等对信息安全要求极高的领域，现有技术尚难以满足其全部需求，使得这些领域的知识产权保护形势更为严峻。

（二）法规框架存在缺陷

信息安全技术在知识产权保护中所面临的另一关键问题，是法规框架的不完善。虽然各国均已认识到信息安全与知识产权保护的重要性，但现行法规在实施过程中暴露出诸多短板。首要问题是，法规制定常常跟不上技术发展的步伐。在面对新兴的网络威胁与错综复杂的侵权手段时，往往缺乏明确的法律支撑。例如，当前的知识产权法律主要应对传统侵权形式，而对于网络空间中的黑客攻击、非法数据共享等行为，法律覆盖存在盲区，保护力度不足。此外，国际间法规的不统一也为知识产权保护带来了难度。在全球化和信息化的今天，知识产权侵权行为往往跨越国界，而各国法律体系的差异导致某些侵权行为在特定国家难以受到应有的惩处，为跨国侵权提供了便利。同时，法律执行难度大也是一个亟待解决的问题。即便存在相关法律，实际操作中，由于证据收集困难、取证成本高昂，许多侵权行为难以及时通过法律手段得到有效处理，侵权者常能逃避法律制裁。再者，法律条款解释与应用的争议性，导致实际案件判决结果的不确定性，增加了知识产权所有者的法律风险和成本。

（三）人员安全意识薄弱与操作不规范

保护知识产权的过程中，信息安全技术所面临的另一大挑战在于人员的安全意识薄弱以及操作上的不规范。即便技术手段再高超，若使用者缺乏必要的安全意识和规范操作，知识产权的保护效果仍将受到严重影响。而众多企业与机构员工对信息安全及知识产权保护的重要性缺乏深刻认识，常常误以为信息安全仅仅是技术部门的职责，从而忽视了自身在日常工作中的安全实践。诸如使用简单密码、密码重复使用，以及在公共网络环境下处理敏感信息等行为，均会极大提升知识产权被盗取的风险。且员工在实际操作过程中的不规范行为也为信息安全埋下了隐患。例如，处理关键文件时不进行加密保护，未按照规定进行数据储存与传输，甚至在离职时未能妥善处置所接触的知识产权信息，这些行为都可能导致知识产权的泄露。此外，员工培训的缺失亦是一个显著问题。许多企业未能定期对员工进行信息安全与知识产权保护的培训，导致员工在面临复杂的网络威胁时，缺乏必要的应对能力，不知有效利用安全技术工具。例如，面对钓鱼邮件、社交工程攻击等常见威胁时，众多员工缺乏识别与防范能力，这极易导致企业的知识产权信息被非法获取。

三、信息安全技术在知识产权保护中的应用策略

（一）加大技术防护力度

为更有效地保护知识产权，必须强化技术防范措施。首要任务是加大先进加密技术的研发和应用。应利用强大的加密算法，例如高级加密标准（AES）和椭圆曲线加密（ECC），以保障数据在传输与存储中的高度机密性。同时，鉴于量子计算技术的进步，需提前规划量子安全加密技术，以预防未来的安全漏洞。同时，必须建立严密的访问控制机制，通过身份认证和权限管理，确保敏感信息仅限授权人员访问。生物识别技术，如指纹识别、面部识别和虹膜识别，能显著提升身份认证的安全与便捷性。此外，零信任架构应作为网络安全的核心原则，所有内外部访问均须经过严格验证与监控。其中，入侵检测和防御系统（IDS/IPS）是技术防护的关键，通过实时监控网络流量和系统行为，迅速识别并阻断潜在威胁。结合大数据与人工智能技术，可提升入侵检测的精确度和响应速度，有效防范高级持续性威胁（APT）。同时，应广泛应用虚拟私有网络（VPN）和安全套接层（SSL）技术，确保远程访问的安全。且数据备份与恢复技术同样重要，应定期备份数据，并在多地保存备份副本，以防数据因硬件故障或自然灾害等意外而丢失。云计算和云存储虽提供了便捷高效的数据备份方案，但云环境的安全防护也需加强，通过数据加密、访问控制和日志监控等手段确保云端数据安全。最后，企业应建立并完善信息安全管理体系，遵循 ISO/IEC27001 等国际标准，不断优化安全策略与措施，确保技术防护的科学性和有效性。

（二）健全法律法规体系

健全法律法规体系是保护知识产权的关键策略。为此，各国应迅速行动，制定并优化与信息安全及知识产权保护紧密相关的法律条文，确保法律能与时俱进，满足科技发展的迫切需求。法律条文必须详尽清晰，全面覆盖加密技术、区块链技术、数字版权管理（DRM）等各类信息安全技术的应用场合，为每项技术的合法应用提供坚实的法律支撑。且国际社会需加强法规的协同与合作，致力于构建统一的国际法规标准和规范，以化解跨国知识产权保护中的法律冲突和执法困境。通过签署双边或多边协议，增进各国在信息安全与知识产权保护方面的协作与互助，联手打击跨国侵权活动。同时，为提升法律执行力，各国应对信息安全和知识产权侵权行为实施更严厉的惩处，构建完备的执法体系。执法

部门应配备专业素养高的技术人员和尖端技术设备，以确保能及时发现、深入调查和妥善处理各类侵权行为。同时，法律应明确规定严厉的处罚措施，对侵权者施以重大的经济和刑事处罚，从而提高侵权成本，形成强大的威慑力。而在法律的保护下，企业与个人也应积极担当信息安全与知识产权保护的责任。法律应明确企业在信息安全方面的基本职责，诸如建立严密的安全管理体系、进行全面的安全风险评估、采取有效的技术防护措施等。同时，法律还应激励企业通过合法渠道维护其知识产权，如申请专利、商标和著作权，并依法解决知识产权争端。为提升法律法规的实效，还需加强普法宣传工作。政府和相关机构应利用多元化的形式和渠道，向公众普及信息安全与知识产权保护的法律常识，从而提升整个社会的法治意识和观念。此外，法律法规的制定与实施应广泛吸纳公众参与，充分听取各方意见与建议，以确保法律法规的科学性、合理性和适用性。

（三）加强人员意识与技能培训

提升员工的信息安全和知识产权保护意识及技能，是确保信息安全技术有效发挥作用、进而保护知识产权的基石。企业应通过持续且深入的培训和教育活动，全面增强员工对信息安全和知识产权重要性的认识。这种培训需覆盖公司各个层级，上至高管，下至基层员工，使每位成员都深刻理解信息安全的核心价值和基础常识。而培训内容应囊括信息安全的基础知识、常见的网络威胁及相应的防范措施，以及应急响应的标准流程，从而帮助员工构建起完备的安全防护意识。此外，针对不同职能部门的特定需求，企业还应提供量身定制的安全培训课程。例如，为研发人员开设关于在产品开发阶段妥善保护知识产权的课程，为 IT 人员提供关于掌握最新安全技术和防护手段的培训。通过组织实战模拟和攻击演练，可有效提升员工在实际工作中应对安全威胁的能力。同时，建立一套完善的安全操作指南和流程也至关重要，这将指导员工在日常工作中正确处理并保护机密信息。这些操作规范应详细涵盖数据加密、访问权限控制、数据备份与恢复等关键环节，确保员工在处理与知识产权相关的信息时，能遵循行业最佳实践。为确保这些规范得到有效执行，企业应定期开展内部审查和审计，及时发现并纠正任何不符合规范的行为。技术人员专业技能的提升同样不容忽视。企业应积极为技术人员创造持续的职业成长机会，如支持其参加 CISSP、CEH 等国际专业认证和培训课程。这有助于技术人员应对日益复杂多变的安全挑战，还能确保企业在信息安全领域保持技术领先。同时，企业内部应建立知识分享和协作的平台，促进技术人员之间的经验交流和技术提升。此外，借助外部专家和顾问的力量，定期进行全面的安全评估和审计，是发现潜在安全隐患并提出针对性改进建议的有效途径。外部专家的丰富经验和专业知识，将为企业优化安全策略和措施提供有力支持，从而提升企业整体的安全防护水平。最后，塑造一种重视信息安全的企业文化也至关重要。企业应将信息安全视为其发展的核心组成部分，并在内部营造一种积极的安全氛围。管理层应通过自身行为树立榜样，将信息安全纳入企业的绩效考核和激励机制中。通过表彰和奖励在信息安全方面表现突出的员工，进一步激发全员对信息安全工作的热情和参与度。

四、结语

综上所述，信息安全技术在知识产权保护中扮演着举足轻重的角色。通过加强技术防护、完善法律法规以及提升员工的安全意识和技能，能有效地迎接知识产权保护所面临的种种挑战。科技的持续进步与法律体系的日益完善将推动信息安全技术更上一层楼，从而为创新成果的合法使用及企业核心竞争力的增强提供坚不可摧的保障。展望未来，企业与政府需进一步深化合作，携手推进信息安全技术的革新与应用，共同打造一个更为安全稳固的知识产权保护环境。

参考文献

[1]张涛.生成式人工智能训练数据集的法律风险与包容审慎规制[J].比较法研究，1–20[2024–07–31].
[2]天津市和平区人民检察院课题组.检察机关深度参与下知识产权综合保护的关系协调[J].山西省政法管理干部学院学报，2024，37（03）：34–39.
[3]孙玉荣，卢润佳.智能时代二次创作的著作权保护与限制研究[J].北京联合大学学报（人文社会科学版），2024，22（04）：45–54.
[4]王超，庞晓敏.RCEP 中的知识产权法规与案例[J].法制博览，2024，（19）：163–165.
[5]贾丽萍.数据知识产权的权利证成与规则展开[J].法制与社会发展，2024，30（04）：205–224.
作者简介：姜靖，男，汉族，1999 年 2 月，陕西宝鸡人，专科学历，西藏熙安信息技术有限责任公司等保测评师，研究方向为网络安全。