DOI：10.13998/j.cnki.issn1002-1248.2020.12.20-0983

基于网络安全等级保护 2.0 的农业科研单位网络安全体系研究——以中国农业科学院为例

王　丹，孙　洋*，谢　辉，张丽萍，万　锋，王燕军

（中国农业科学院 农业信息研究所，北京　100081）

摘　要：［目的 / 意义］大数据时代，中国农业科研单位持续加强信息化建设，给科学研究和科研管理带来极大的便利，但相应的信息安全问题也开始逐渐显现。依托信息等级保护工作，深入分析农业科研单位信息系统建设中各个薄弱环节，提高信息系统安全，避免发生网络安全事件已被摆在农业科研单位工作的突出地位。［方法 / 过程］按照等级保护制度要求，论文主要围绕加强农业科研单位信息安全管理的内容进行探讨，介绍了信息等级保护的重要性，对比分析了等级保护 2.0 标准与等级保护 1.0 标准的不同；详细分析中国农业科学院的网络安全管理制度体系和网络安全管理技术等内容，最后对加强农业科研单位信息安全建设的有效策略提出了相关建议。［结果 / 结论］论文以中国农业科学院为例详细论述其相关做法，希望为各农业科研机构开展网络安全等级保护安全建设提供借鉴。

关键词：网络安全；等级保护 2.0；安全技术；安全管理；安全策略

中图分类号：G322；C932　　**文献标识码：**A　　**文章编号：**1002-1248（2020）12-0097-07

引用本文：王丹，孙洋，谢辉，等. 基于网络安全等级保护 2.0 的农业科研单位网络安全体系研究——以中国农业科学院为例[J]. 农业图书情报学报，2020，32(12)：97-103.

Network Security Systems of Agricultural Research Institutions Based on Hierarchical Protection 2.0: Taking the Chinese Academy of Agricultural Sciences as an Example

WANG Dan, SUN Yang*, XIE Hui, ZHANG Liping, WAN Feng, WANG Yanjun

(Department of website system, Agricultural Information Institute of CAAS, Beijing 100081)

Abstract: [Purpose/Significance] In the era of big data, agricultural research institutions in China have begun to in

收稿日期：2020-10-29

基金项目：中国农业科学院基本科研业务费专项“农业科技创新联盟云视频协同平台和新媒体融合门户关键技术研究与运维”（Y2020LM07）

作者简介：王丹（1972-），女，硕士，副研究员，研究方向为信息化研究、信息系统应用。谢辉（1978-）男，助理研究员，研究方向为信息系统应用。张丽萍（1975-）女，副研究员，研究方向为信息安全管理制度研究。万锋（1970-）男，助理研究员，研究方向为信息化研究、数据安全。王燕军（1969-）男，助理研究员，研究方向为数据治理

*通信作者：孙洋，女，硕士，研究方向为信息化研究、信息系统应用。Email：sunyang@caas.cn

DOI：10.13998/j.cnki.issn1002-1248.2020.12.20-0983

crease the investment in informatization construction to bring great convenience to scientific research and management, but corresponding information security issues have risen to the surface. Tasks such as relying on the network hierarchical protection and performing in-depth analysis of each weak link in the information system construction of agricultural research institutions to improve the information system security and avoid network security problems have been placed in a prominent position in the work of agricultural research institutions. [Method/Process] This article discusses the issue of strengthening the information security management of agricultural research institutions based on hierarchical protection 2.0. First of all, this article introduces the importance of hierarchical protection. Secondly, the difference between hierarchical protection 2.0 standard and h1.0 standard is analyzed. Thirdly, the system of network security management and the network security management technologies of Chinese Academy of Agricultural Sciences were analyzed in detail. Finally, it discusses and summarizes the effective strategies to strengthen the information security construction of agricultural research institutions. [Results/Conclusions] Taking the Chinese Academy of Agricultural Sciences as an example, this paper discusses its practices in detail, in the hope of providing reference for agricultural research institutions to carry out network security hierarchical protection.

Keywords: network security; hierarchical protection 2.0; safety technology; safety management; safety strategy

1 引 言

中国农业科学院是国家级综合性农业科研机构，担负着中国农业重大基础研究、应用研究和高新技术研究的任务。中国农业科学院信息化建设经过多年的不断发展，院信息化在基础设施和学科领域应用等方面取得了长足的进步。目前院级网络核心机房建有500m²B类标准机房。京内中关村院区已实现“万兆主干，千兆桌面”网络环境，核心网络出口带宽3.4Gbps。依据“统一架构、集中认证、分级管理、开放兼容的”原则建设了“CAAS”无线网络，实现与Eduroam联盟对接。构建了云计算基础设施环境“农科云”平台（一期），达到170T存储、250T备份能力，为195个业务系统提供服务。全院运行着包括“1+36”院所两级门户网站群平台、智慧农科协同平台、数字农科院系统1.0、电子邮件系统、CAAS云会务、CAAS云视频、CAAS云文档等信息化应用系统。伴随着上述信息化应用系统的全面上线，逐渐形成了一个服务于全院职工、研究生院在校学生的重要综合性网络。

但我们也看到，承载中国农业科学院重要业务系统安全防护手段却仍然相对落后。当前信息安全形势复杂多变，在数字化转型过程中，物联网、大数据、人工智能和云计算等新兴技术的应用，导致外界对中国农业科学院的攻击对象、攻击方式、攻击领域不断扩大，传统的网络边界持续瓦解，带来物联网安全、云安全、移动安全、数据安全、安全智能运维等全新的挑战，这些问题制约了中国农科院信息化支撑能力建设，让全院的信息安全防护与管理的压力愈来愈大。中国农业科学院根据国家相关要求，在现有网络架构下对中关村院区的核心网络、重要公共业务系统进行了安全整改与加固，提升了网络与应用系统的风险防护、动态防御、主动防御的能力。

2 网络安全等级保护的重要性与基本概念

随着信息技术的不断应用，给科研单位科研和管理带来极大便利的同时，同时也带来了信息安全方面的隐患。例如，2017年6月1日《中华人民共和国网络安全法》正式实施后的第一案，宜宾市翠屏区“教师发展平台”网站2017年7月22日发生被黑客攻击入侵的网络安全事件，教师个人信息泄露，造成了极

坏的社会影响。由此可见，网络安全、信息安全是何等重要[1]。中国农业科学院是国家级农业科研机构，它的稳定发展对人民的生活、社会的稳定性起到至关重要的作用。因此，加强中国科研领域的信息安全管理对推进中国的信息化建设具有十分重要的意义。

2019 年 5 月，国家发布《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》《信息安全技术网络安全等级保护安全设计技术要点》3 个网络安全领域的国家标准，标志着等级保护 2.0 的正式到来，并于 2019 年 12 月 1 日，等级保护 2.0 标准正式实施。

等级保护 2.0 是顺应当前加强网络安全的国家要求，结合云计算、移动互联、物联网、工业控制和大数据等新技术新应用开展综合治理、系统监管、主动防控的时代。下表为等级保护 1.0 标准与 2.0 标准对比[2]。

表 1　等级保护 1.0 标准与等级保护 2.0 标准对比表

	等级保护 1.0 标准	等级保护 2.0 标准
等级保护对象	信息系统	基础信息网络
		信息系统
		大数据平台
		云计算平台
		物联网
		工业控制系统等
管理部分	安全管理制度	安全策略与安全制度
	安全管理机构	安全管理机构与人员
	人员安全管理	安全建设管理
	系统建设管理	安全运维管理
	系统运维管理	
技术部分	物理安全	物理和环境安全
	网络安全	网络和通信安全
	主机安全	设备和计算安全
	应用安全	应用和数据安全
	数据安全及备份恢复	

由表 1 中看出，等级保护 2.0 标准的保护对象由单一的信息系统扩大为信息系统、基础信息网络、大数据平台、云计算平台、物联网、工业控制系统等，将近年来新兴领域全部纳入，构成了“安全通用要求 + 新型应用安全扩展要求”的安全要求。技术部分分类框架更加统一，形成了“安全通信网络”“安全区域边界”“安全计算环境”和“安全管理中心”支持下的四重防护体系架构。各个环节强化了可信计算技术使用的要求，逐级提出各个环节的主要可信验证要求。可以看出，等级保护 2.0 的目标是建立“打防管控”一体化的网络安全综合防御体系，提升国家网络安全整体防御能力；变被动防护为主动防护，变静态防护为动态防护；重点保护关键信息基础设施、重要信息系统和大数据安全。

3　中国农业科学院网络安全等级保护的基本内容

随着信息技术的快速发展，中国农业科学院加快信息化建设进程。但在信息技术应用过程中，很可能会出现信息安全问题，从而造成单位重要信息被窃取、被破坏、被篡改等情况。

中国农科院按照网络安全等级保护要求，以中国农业科学院门户网站和中国农业科学院所级门户网站群系统等院级重要业务系统为切入点，围绕院级业务系统开展等级保护定级备案、建设整改和等保测评工作，充分分析业务系统的特点，从安全防护的难点入手逐一进行解决，通过安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理人员、安全机构管理等建立和完善，切实提高了院网络、业务系统安全防护能力、隐患发现能力、应急处置能力，为院信息化的健康发展提供可靠保障。

通过上述建设与实施，中国农业科学院门户网站系统顺利通过等级保护 2.0 标准下的等级保护三级系统测评，取得良好成效。

中国农业科学院网络安全等级保护体系包括网络安全管理制度和网络安全技术两部分内容。

3.1　网络安全管理制度体系的内容

中国农业科学院信息安全管理制度体系建设通过现状调研分析、信息安全管理体系规划设计、信息安

DOI：10.13998/j.cnki.issn1002-1248.2020.12.20-0983

全管理制度落地三大阶段，最终形成了中国农业科学院信息安全管理制度体系（图 1）。信息安全管理制度是保证信息安全的基础，信息管理的目的是让参与信息安全的所有人员都能够按照确定的要求去行动。通过一系列规章制度的实施，来确保各类人员按照制度规定的职责行事，防止恶意侵犯，避免安全责任事故的发生[4,5]。

中国农业科学院信息安全管理制度主要包括 4 个层面，第一层面是纲领性的文件，是信息安全各领域的总体策略，解决的是“为什么”的问题。第二层面是规范、程序、管理办法，是信息安全各领域的具体要求，解决的是“做什么”的问题。第三层面是细则、指南、手册。是信息安全各领域的详细做法，解决的是“怎么做”和“做到怎样”的问题。第四层面是记录、表单。是信息安全政策和标准的实际执行结果的痕迹，解决的是“做的结果”的问题[6,7]，详见图 2。

中国农业科学院信息安全管理制度包括 23 项管理制度，4 项操作规范和 34 项执行表单，如表 2 所示。

中国农业科学院通过信息安全管理制度体系的建立和执行，进一步加强了以下内容。

3.1.1 强化网络安全工作方针和策略

中国农业科学院通过进一步明确全院信息安全总体目标和策略，制定信息安全总体规划和实施路线，规范细化网络信息安全工作方针和策略。对重要业务

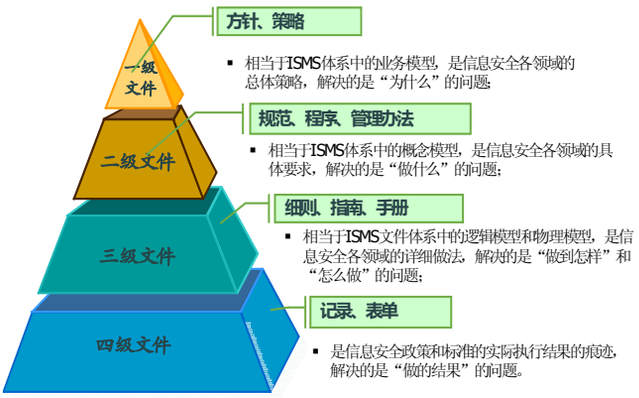

图 2 中国农业科学院信息安全管理制度体系构成图

系统采用分区分域、等级防护；对信息安全人员录用、转岗、离职进行规范化管理[8]；对系统建设的需求设计、系统开发、测试、上线验收全生命周期进行安全化管理；对运维过程中各节点实行安全管控。从而有效保障了中国农业科学院网络安全工作顺利实施[9]。

3.1.2 明确安全网络安全主体责任制

中国农业科学院成立了网络安全和信息化领导小组，领导班子主要负责人为领导小组组长，下设管理部门。每年制定网络安全年度工作计划并确保执行[10]。本着“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，厘清责任，建立院本级与院属各单位党委党组领导下的网络安全责任制，把网络安全责任制纳入各单位考核机制，发生重要网络安全事件实行一票否决。层层压实各单位网络安全主体责任[11]。

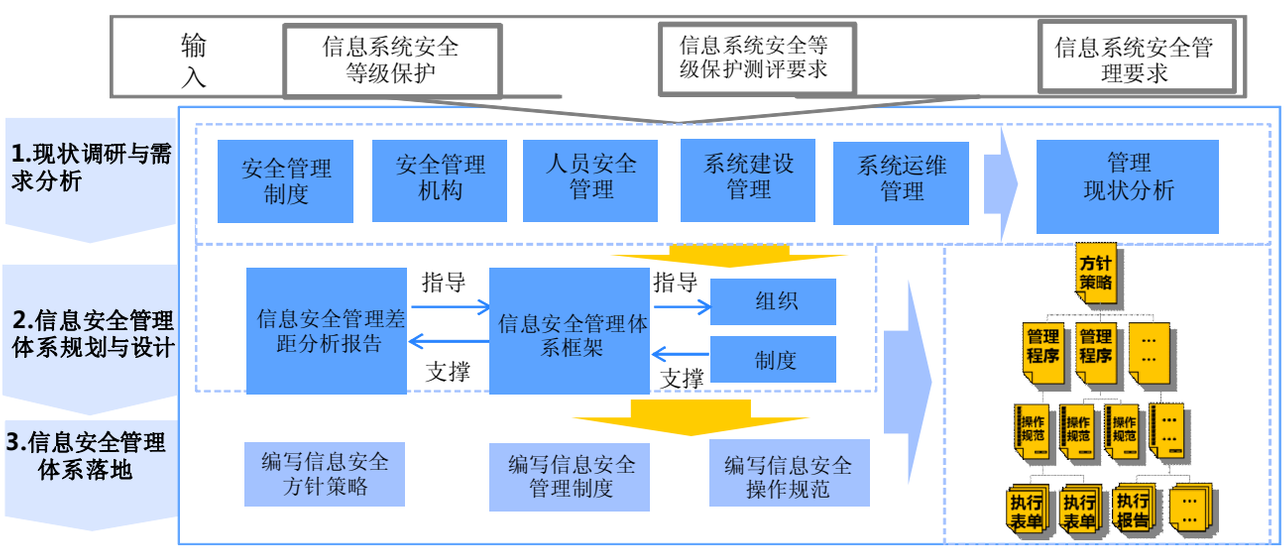

图 1 中国农业科学院信息安全管理制度体系技术路线图

表 2 中国农业科学院信息安全管理制度汇总表

文件层级	管理域	文件数量/个
一级文件	信息安全工作方针和策略	1
二级文件	文档管理制度	22
	安全管理机构	
	信息安全组织体系和职责	
	岗位职责管理制度	
	人员安全管理	
	人员安全管理制度	
	信息安全检查管理制度	
	系统建设管理	
	产品采购和使用管理制度	
	信息系统软件开发管理制度	
	代码编写安全管理制度	
	信息化项目建设管理制度	
	信息系统等级保护管理制度	
	系统运维管理	
	机房安全管理办法	
	办公环境管理制度	
	资产安全管理制度	
	……	
三级文件	网站内容管理系统用户使用手册	4
	操作系统安全配置规范	
	数据库安全配置规范	
	中间件安全配置规范	
四级文件	安全管理检查表格	34
	安全技能和安全认知考核记录	
	……	

3.1.3 人员培训常态化

网络安全等级保护工作需要绝对专业的技术人员长时间持续进行，但目前中国农业科学院从事信息安全工作的人员工作经验少且技能欠缺，因此单位每年制定培训计划，对安全相关人员进行信息安全知识和技能培训，使其尽快掌握相应的技能，提高单位的网络信息安全保障能力[12,13]。

3.1.4 信息安全事件应急处理

面对日益严峻的网络安全环境，提前制定信息安全突发事件的应急预案十分必要。中国农业科学院采取预防与处理相结合，以预防为主[14]。根据系统中断时长、影响范围，以及数据丢失或被篡改、窃取对国家和社会稳定构成威胁的严重程度或经济损失进行事件等级划分。加强风险排查，提前做好应急处理的各项预案，严格执行监控值守制度，确保及时发现故障，保证 7*24 小时应急响应[15]。

3.2 信息安全技术内容

3.2.1 信息数据安全

中国农业科学院长期积累的数据已成为单位的最宝贵财富之一，因此需要针对重要数据进行重点保护[16,17]。对院级关键业务系统数据至少每个工作日备份一次；备份数据保存期不低于 6 个月。不断完善数据备份恢复机制，定期对备份数据进行有效性验证，确保数据的完整性、可用性，避免因数据丢失给单位造成无法弥补的损失。但因条件有限，没有采用数据同城或异地备份。

3.2.2 业务应用安全

从业务需求和系统安全角度出发，对院级重要系统涉及的网络设备、安全设备、服务器和数据库启用身份标识和鉴别模块。制定应用访问控制策略、访问权限[18]。及时修补系统漏洞，做好院级重要系统监控和安全审计。对业务系统管理员权限遵循最小授权原则。每月进行一次漏洞扫描，及时修补安全漏洞。在测试环境中安装安全补丁并测试通过，避免直接在正式环境安装，确保业务应用安全[19]。

3.2.3 通信网络安全

中国农业科学院通信网络具有覆盖面积大和节点多的特点，是单位信息化工作的重中之重。已根据业务情况划分不同网段，对重要网段进行重点保护[20]；核心交换机、防护墙、重要业务系统前台服务器、数据库服务器均采用冗余设计。外网访问内网资源使用 VPN 远程登陆，保证数据在传输过程中的安全性。实行 7*24 小时网络监控；重要网络结点保存至少 6 个月日志记录；定期对日志进行分析，发现异常及时处理。使网络的安全性和运行效率得到提升[21]。

3.2.4 计算环境安全

中国农业科学院对所有服务器进行密码设置，每 3

DOI：10.13998/j.cnki.issn1002-1248.2020.12.20-0983

个月更换一次密码，密码具备复杂度。定期进行网络杀毒和漏洞扫描，关闭不必要的服务端口[22]。按照最小服务原则进行安全配置，开启相应的安全审计功能，对服务器等进行监控，确保其安全运转。各设备及操作系统采用安全协议远程管理。

3.2.5 区域边界安全

中国农业科学院按照等级保护的要求，对不同网络区域采用不同防护策略。例如等级保护三级系统区域部署了 IPS 设备、WAF 设备，对入侵行为进行监测；部署了 WEB 应用防火墙，制定合理网络安全访问策略[23]；同时设置必要的堡垒机、安全审计设备、安全管理平台、日志审计等网络安全设备，从而使等级保护三级系统区域网络安全的高可用性得到较好的保障。

3.2.6 物理环境安全

中国农业科学院中关村院区核心网络机房的物理环境满足了双路供电、UPS 电源，远离水源与电磁干扰等要求，达到 B 类机房标准；做好核心网络机房的监控、报警、消防、防雷击、防静电、供电保护等工作，确保其场所的安全性。同时严格设置机房值班管理，专人值守。严格设立相应的门禁和访问控制措施，对人员的进出进行登记与监管，为业务系统的稳定运行提供可靠的物理环境。

4 加强科研单位信息安全建设的有效策略建议

中国农科院网络安全等级保护研究建设对农业科研单位网络安全建设具有普遍借鉴意义，因此对科研单位网络安全等级保护建设提出如下策略建议。

4.1 完善单位的安全管理机构和管理制度

建立健全安全管理机构和严格落实管理制度对保证科研单位信息安全起到压舱石的作用。科研单位的信息安全管理机构由决策机构、管理机构和执行机构组成。这种 3 层安全管理机构的架设，利于逐级明确每个单位、每个岗位的相应职责，压实主体责任。同时科研单位要建立和完善安全管理制度，并严格组织落实。以上两方面对促进科研单位信息安全建设意义非常重大[24]。

4.2 加大信息安全投入

多年以来，农业科研机构在信息安全防护方面投入的资金少之又少，从而造成了安全隐患。在规划和建设信息系统时，安全防护措施应按照“三同步”原则，即与信息系统建设同步规划、同步建设、同步投入运行，把信息安全防护措施贯彻始终。

4.3 加强专业化人才的引进与培训

信息安全管理工作需要相当专业的技术人才，因此科研单位在人才引进与培训要做到以下两点：第一，严格对引进专业技术人才进行资格审查，关键岗位应具备能证明其业务能力的如 CISP 或 PMP 证书[25]。决定录用后，要与单位签订保密协议；离职时，应及时收回所有访问权限、证件及使用的软硬件设备。第二，科研单位应至少每年对业务人员进行一次培训和考核，逐步提高业务人员的安全技能和安全意识。

4.4 加强科研数据安全保护

科研单位长期积累的数据已成为单位的最宝贵财富之一。农业科研数据多为实验数据、监测数据、图像数据等，动辄几百 GB，甚至上 T，课题组没有那么大的空间去备份，基本就是存储在课题组的服务器上，这存在极大的安全隐患。正规数据备份多采用数据库备份、网络数据备份、磁带备份和镜像备份。应根据数据的重要程度，制定适合单位的数据备份策略，提供重要网络设备、通信线路和服务器的硬件冗余。防止因系统故障导致数据丢失，造成无法弥补的损失。

5 结　语

大数据时代下，中国农业科研单位正在朝着信息化方向迅速迈进，同时也面临着信息安全的严峻挑战。农业科研单位正逐渐加强对网络安全等级保护的重视，不断从实践中总结经验，实现自身网络安全保护措施

的进一步完善，从而使中国农业科研信息安全保障水平得到明显提高。

参考文献：

[1] 杨春, 徐玮, 夏平平. 基于网络安全等级保护的信息系统安全设计[J]. 现代工业经济和信息化, 2019, 9(11): 68–69.

[2] 何占博. 我国网络安全等级保护现状与 2.0 标准体系研究[J]. 信息技术与网络安全, 2019(3): 9–19.

[3] 栾泉中, 张至柔, 吴娟. 基于等级保护的高校信息系统测评及整改[J]. 办公自动化杂志, 2019(4): 26–28.

[4] 周大勇. 基于等级保护的校园网络安全规划设计方案[J]. 福建电脑, 2019(3): 126–128.

[5] 余兆明. 医院信息系统信息安全等级保护的实施探讨[J]. 网络安全技术与应用, 2019(3): 150–151.

[6] 曾萨. 档案信息系统云安全等级保护需求与策略[J]. 档案管理, 2019(6): 30–33.

[7] 邹鹏. 东北财经大学网络安全加固方案设计与实践[J]. 中国管理信息化, 2020(3): 161–162.

[8] 张辉. 基于网络安全等级保护 2.0 的高校网络安全体系研究[J]. 校园网络安全, 2020(3): 83–84.

[9] 傅钰. 网络安全等级保护 2.0 下的安全体系建设[J]. 网络安全技术与应用, 2018(8): 13–16.

[10] 刘俊. 关于网络安全等级保护 2.0 的探讨[J]. 减速顶与调速技术, 2019(2): 5–6.

[11] 王昭群. 浅析事业单位网络安全等级保护的建设[J]. 行业与应用安全, 2019(7): 118–119.

[12] 郑国伟. 基于网络安全等级保护 2.0 的医院网络研究[J]. 信息网络安全, 2019(10): 76–79.

[13] 段忠祥. “等级保护”背景下智慧校园网络数据安全问题研究[J]. 网络安全技术与应用, 2020(9): 88–90.

[14] 刘刚. 基于等级保护 2.0 的铁路网络安全技术防护体系研究[J]. 铁路计算机应用, 2020(8): 19–23.

[15] 郭乐. 网络安全等级保护 2.0 体系下的法院网络安全管理及应对[J]. 网络安全技术与应用, 2020(5): 136–137.

[16] 袁慧. 网络安全等级保护 2.0 制度的研究和探讨[J]. 信息与电脑(理论版), 2020(1): 223–224.

[17] 马力. 网络安全等级保护 2.0 国家标准解读[J]. 保密科学技术, 2019(7): 14–19.

[18] 张旭辉. 关于网络安全等级保护 2.0 在政务云中的应用研究[J]. 数字通信世界, 2020(6): 240–241.

[19] 陈旭壮. 网络安全等级保护 2.0 安全体系构建[J]. 中国新通信, 2019(22): 76–77.

[20] 张振峰. 网络安全等级保护 2.0 云计算安全合规能力模型[J]. 信息网络安全, 2019(11): 1–7.

[21] 朱岩. 网络安全等级保护下的区块链评估方法[J]. 工程科学学报, 2020(10): 1267–1285.

[22] 李云飞. 网络安全等级保护 2 0 工业控制系统安全测评实践[J]. 网络安全技术与应用[J]. 2020(9): 21–23.

[23] 冯凯亮. 铁路网络安全等级保护管理系统研究[J]. 铁路计算机应用, 2020(8): 66–70.

[24] 张彦. 基于等级保护思想的网络安全风险评估关键技术研究[J]. 铁路计算机应用, 2020(8): 28–32.

[25] 张小林. 高校网络安全等级保护建设研究[J]. 电脑知识与技术, 2020(22): 71–73.