定密工作数字化管理系统设计报告

武自厚　　20336014　　保密管理

一、　引言

随着信息技术在保密管理领域的广泛应用，越来越多的高新技术运用到国家秘密的定密管理中来，其中一个重要的技术即是定密工作数字化管理系统。定密工作数字化管理系统将公文起草、定密、审核、签发、统计、日常管理等功能融为一体，充分利用计算机信息技术快速、高效、准确的优势，通过技术手段实现了强制性规范的定密流程。在一些地方，定密工作数字化管理系统已经在定密工作中投入使用并获得了不低的成效[1]。本文将基于《定密理论与实务》课程内容设计一种定密工作管理系统的机制。

在本文的第二部分，将会从定密依据、定密授权、定密责任人、国家秘密确定、定密监督等概念分模块阐述系统设计。而在第三部分将会选取几个定密工作中经常出现的场景，作为该定密工作管理系统功能的展示。

二、　模块设计

1.　定密依据规范模块

定密依据是定密工作的基础。此模块会存储该工作单位所涉及领域的《国家秘密事项一览表》，并在定密时强制要求定密工作人员选择相应的事项进行定密，便于管理以及后续监督。通过定密条款的选择，系统将会对定密人员在密级、保密时间以及知悉范围进行自动限制。

每一项定密条款都对应着唯一编号存储于系统中。在选择事项中可以实时对事项的具体内容进行查阅，辅助定密工作人员及时把握定密的规则。

目前有一些可以通过文本匹配辅助定密依据查找的技术[2]，在确定国家秘密的过程中，系统将会自动分析文本内容预测合适的定密条款。该模块也会基于文本匹配技术自动在《国家秘密事项一览表》改变自动查询其他工作单位的《国家秘密事项一览表》，如果发现近似或冲突的事项，将会通过信息通知模块向产生冲突的单位发送通知，协助多单位之间会同解决冲突问题。

2. 定密权限管理模块

该模块着重于各个部门、单位之间的定密授权管理，将整个部门、单位视作一个用户。

该模块会记录保密行政管理部门根据《国家定密管理暂行规定》编制的三类定密授权机关名录，将所有定密工作涉及的机关分为“中央国家机关”“省级机关”“设区的市、自治州一级的机关”以及只能获得派生定密权的“被授权机关”四类。每一个机关都会根据其定密权限被分配一个特定的“电子证书”。

在机关进行定密工作时，该模块会自动验证“电子证书”，没有“电子证书”的机关无法选择任何定密条款进行定密，而特定的“电子证书”可以“解禁”特定的定密条款。

被归类为“被授权机关”的机关在需要提交定密授权申请时，该模块将会根据文本匹配技术分析机关所属的行业以及业务内容，匹配一个最合适的定密授权主体机关发送定密授权申请。

具有派生定密权的机关可以主动向“被授权机关”分配“电子证书”以完成定密主动授权。“被授权机关”也可以根据自身业务特点适时申请定密授权，申请时该模块会自动分析机关的业务，生成定密授权申请表。授权机关审核并通过此次申请后将会在此模块记录被授权机关的唯一标识，并自动在相应的保密行政管理部门进行备案。

在机关撤并时自动失去被授权定密的“电子证书”，新成立的机关需要重新通过该模块获得定密授权。

3. 定密责任人模块

上一个模块管理好机关之间的授权问题的同时，该模块着重于单个机关内定密责任人的管理。同一个机关内的定密工作人员会被归类为“法定定密责任人”“指定定密责任人”“承办人”三类。与保密授权模块相似，系统也会给每个定密人员分配特定的“电子证书”来进行识别。为了防止他人擅自冒用身份，系统采用硬件加密狗（必要时采用虹膜、指纹、声纹等生物识别技术）验证定密责任人或承办人的身份。

定密权能够得到规范和效益最大化的关键在于定密的专职化、规范化以及权责一致[3]。而该模块主要采用对定密依据使用的限制来规范定密责任人进行定密的流程。

根据《中华人民共和国保守国家秘密法》第十二条的规定，系统自动将机关、单位的负责人视作法定定密责任人。法定定密责任人可以使用该机关、单位有权使用的所有定密依据。法定定密责任人可以通过该模块进行定密责任人的指定工作。指定时首先需要向系统导入经过认证的候选人的保密培训成绩以及定密培训成绩，只有达到一定水平才能继续；指定时需要法定定密责任人选定一些定密依据的范围（且不超过其本身所能使用的范围）进行指定。指定后系统将会自动向同级保密行政管理部门进行备案，并在本机关、单位内进行公示。

定密责任人在系统中具有以下权限：

- 代表机关申请定密授权。
- 审核承办人的操作。
- 通过“电子证书”在自己职权范围内进行定密。
- 对拟公开信息进行保密审查。
- 提出定密异议。
- 系统内容可能发生泄露时及时收到通知。

4. 国家秘密确定模块

这是定密中最为关键的模块，其主要功能即是将承办人草拟的拟定为国家秘密的公文进行定密。首先根据定密责任人模块的限制，只有定密责任人可以使用这个功能，承办人只能预先填报国家秘密确认表再交由定密责任人审核，且根据定密授权模块以及定密依据模块的限制，定密责任人只能选择自身权限范围内的密点、密级、时限、定密依据及知悉范围。其中知悉范围的选择将会借助本系统中对于机关、单位以及工作人员的唯一标识机制，知悉范围将标识为一系列唯一标识组成的集合，具体到机关、单位、部门甚至是单个工作人员。

该模块集成了自然语言分析程序，辅助定密人员进行国家秘密的确定。模块中可以使用机器学习技术中鲁棒性、准确性以及泛用性都较为显著的最大最小支持向量机（M^3-SVM）技术处理草拟文本[4]。根据对草拟文本的分析，模块将会对密点、密级、知悉范围、定密依据以及保密时长进行建议。介于机器学习技术本身具有一定的局限性，最终定密结果依然需要定密责任人在了解系统建议后自行作出选择，尊重定密责任人的主观能动性。

在定密责任人无法确定时，可以将此次定密请求提请上级主管部门或者同级保密行政管理部门解释相关条款进行答复，此时系统会生成有争议事项定密申报表。申报定密时系统会自动生成不明确事项定密申报表。对于本单位无定密权的事项，承办人应当向在系统中填写无权定密事项定密申报表，系统将自动发送至上级主管机关、单位或业务主管部门、保密行政管理部门，并在规定期限内批复。

定密审批完成后，文件正式成为国家秘密，系统自动生成密级表示以及审批单进行备案。随后国家秘密交由定密后模块进行管理。

5. 定密后管理模块

国家秘密的确定不代表定密工作的结束，而这之后的工作主要由该模块完成。

在本单位定密的国家秘密将会按照级别存储于“绝密库”“机密库”“秘密库”三个数据库中，并按照《中华人民共和国密码法》的规定，“绝密库”采用核心密码加密，“机密库”“秘密库”采用普通密码加密。如果有成员试图访问、写入或打印，模块将会验证国家秘密的知悉范围以及成员的唯一标识的“电子证书”，如果“电子证书”验证为不通过，系统将拒绝操作并记录此次验证。

除此之外对于实际工作中国家秘密可能发生变化，因此还有“定期审核库”“待解密库”两个特殊的国家秘密数据库。

即将进行年审的国家秘密会在“定期审核库”中产生一个引用（即其本体依然分级保存在前面介绍的三个数据库中），定密人员需要审核库中的国家秘密。如果需要变更，则需要承办人在系统填写《国家秘密变更审批表》，经由定密责任人审核通过后，系统自动变更密级标识、生成国家秘密变更标志，并且发出指令使所有新的知悉范围内单位的保密管理信息化系统能够浏览的此项国家秘密同步为最新状态。如果需要审查解密，则需要承办人在系统填写《国家秘密解密审批表》，经由定密责任人审核通过后，系统自动消除密级标识、作出国家秘密解除标志并发出通知告知原知悉范围内的所有机关、单位。上级机关、单位具有查看并操作下级的“定期审核库”

即将到达保密期限的国家秘密转送至“待解密库”，定密责任人可以进行查看。如果没有任何操作，此库将会在保密期限到期时自动解密，消去密级标识并将记录备案。

6. 定密监督模块

该模块负责进行定密监督。

上级机关、单位可以启动专项检查，通过主动浏览下级国家秘密数据库，检查其中的记录是否符合规范；该模块也具有定密抽查功能，随机随时抽取下级单位的国家秘密确定/变更/解除记录供上级机关、单位浏览并审查。在检查中如果发现问题，上级机关、单位通过系统发起定密纠错，既可以通知下级机关、单位定密责任人，必要时也可以直接通过该系统获取更改出现错误的国家秘密的权限。

该模块还会将本机关、单位所有定密记录进行收集和分析，定期形成报表，供定密责任人以及上级机关、单位查看审核。

该模块提供定密异议功能，定密责任人可以向原定密机关、单位提交定密异议，系统会将此异议告知原机关、单位进行决定。如果不服原机关、单位的决定，还可以通过系统报相关保密行政管理部门处理。

该模块具有审计功能，可以自动记录所有系统中的操作记录，一旦泄密事件发生，即

可通过查询系统记录发现是在哪一个环节出现了问题。对于异常、反常的权限验证，系统会及时记录并报警。

7. 信息定向传输模块

定密管理中少不了各个机关、单位之间的协助，而此模块则实现了这方面的功能。

首先是通知类信息的传输，在进行定密授权、定密监督、国家秘密的确认/变更/解除时，系统都会调用此模块通知知悉范围内的机关、单位及其定密责任人。

其次是“电子证书”的发放，在进行定密授权或者批准无权定密定密申请时需要上级机关、单位分发长期或临时的“电子证书”，在发放过程中，系统会根据《密码法》相关规定使用核心密码或普通密码或商业密码加密“电子证书”本身，并在收到“电子证书”时进行验证，如果发现被篡改则实时进行报警。

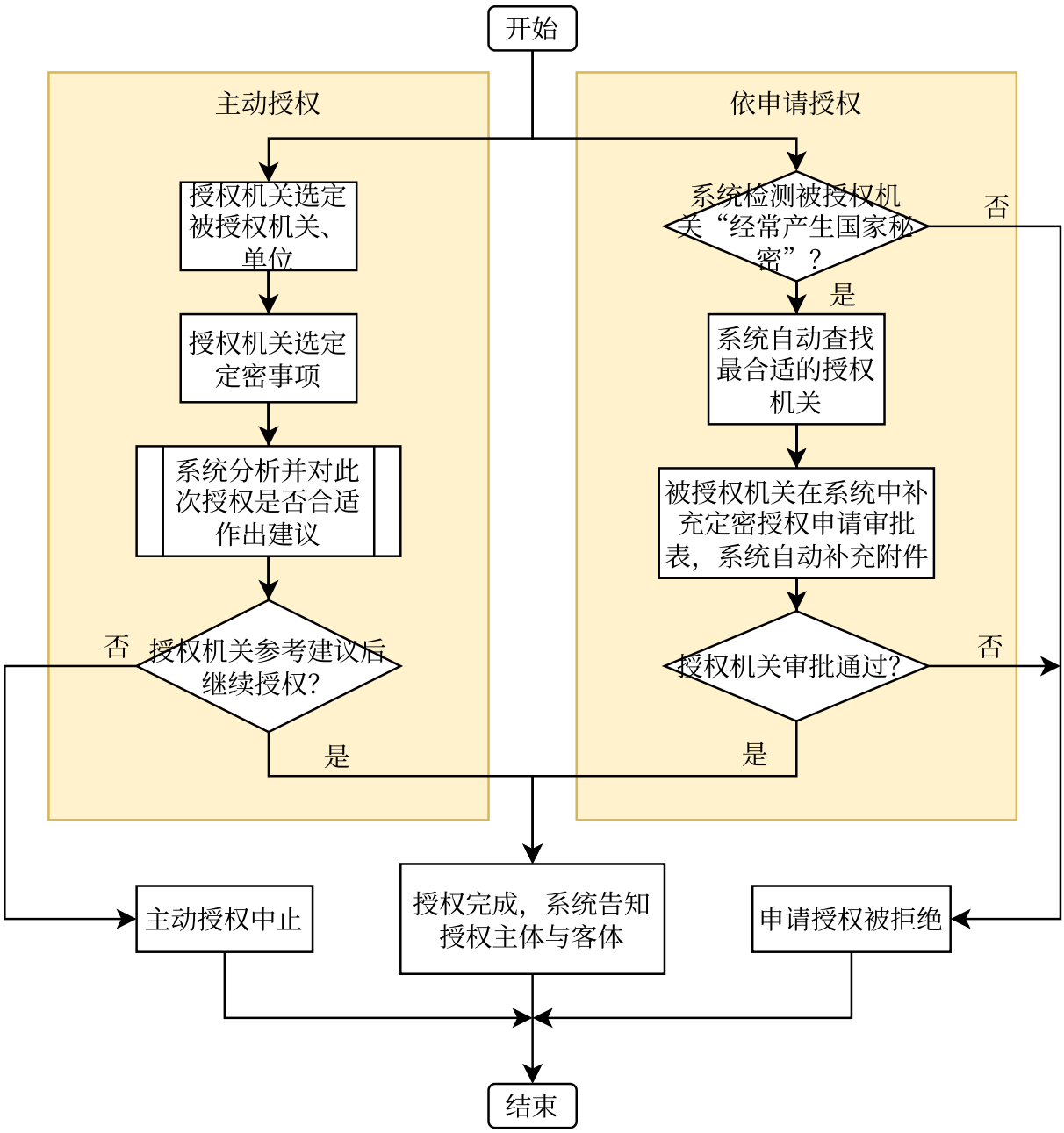
最后是知悉范围内国家秘密的查看。为了安全起见，国家秘密不会在系统内创建副本，知悉范围内的保密人员若需要查看，必须通过由《密码法》规定的指定密码加密的内网连接远程查看，查看的时间和设备都会进行记录。国家秘密数据库不允许向外写入任何内容，因此这是一个单向数据流。

在涉及高权限向低权限的授权或写入时，必须由定密责任人确定阅读并遵守《保密承诺书》[5]。模块对外接设备的管理非常严格。所有传输数据的外设必须经过“三合一”安全系统处理。外接设备只有读取系统而不被授予写入的权限，从根本上杜绝了计算机病毒的侵入。

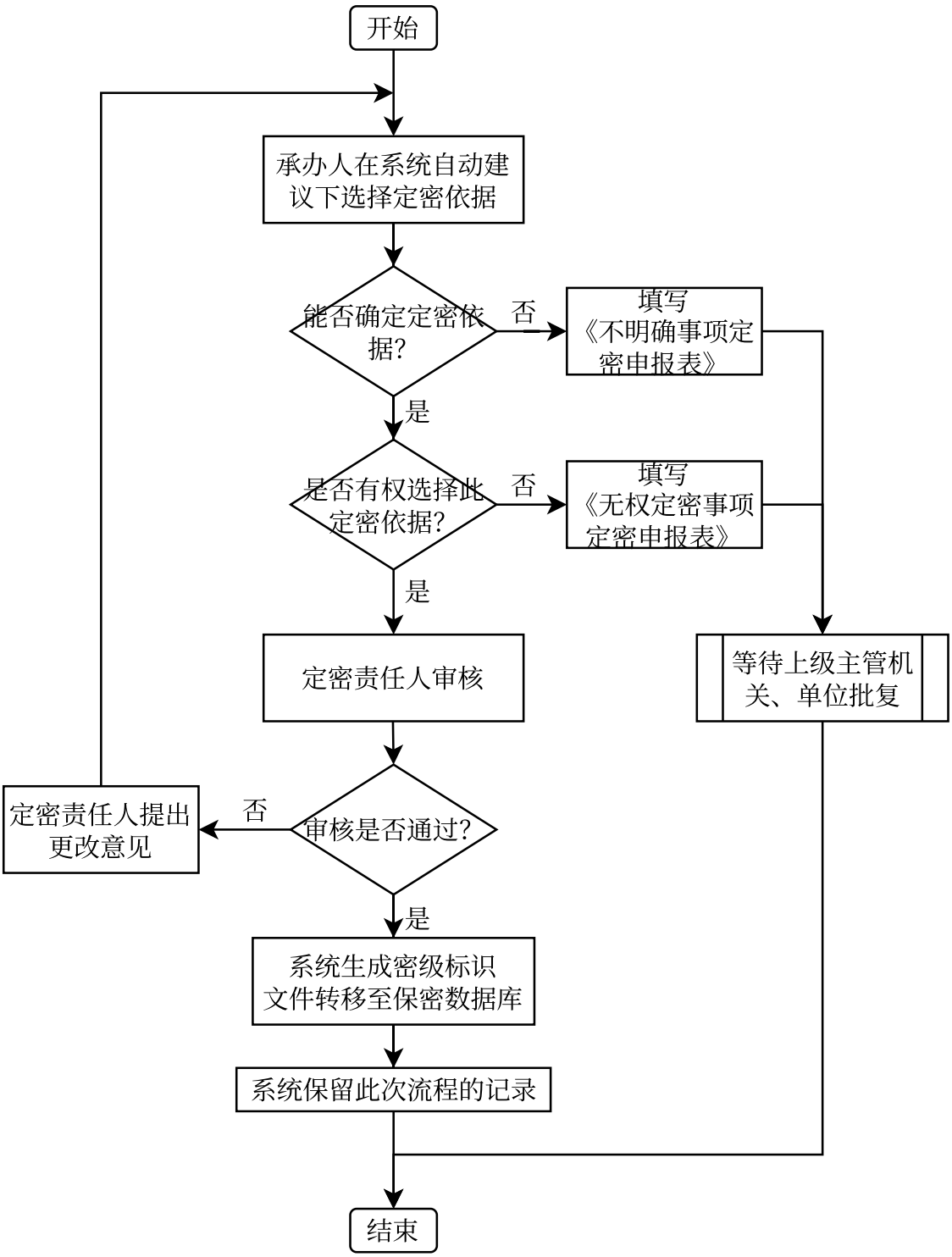
三、 流程示范

在上一个部分介绍系统中各个模块的功能后，本部分将以流程图的形式重点展示定密人员在定密工作中最为重要的定密授权、国家秘密的确定以及国家秘密的定期审核三项工作中的流程。

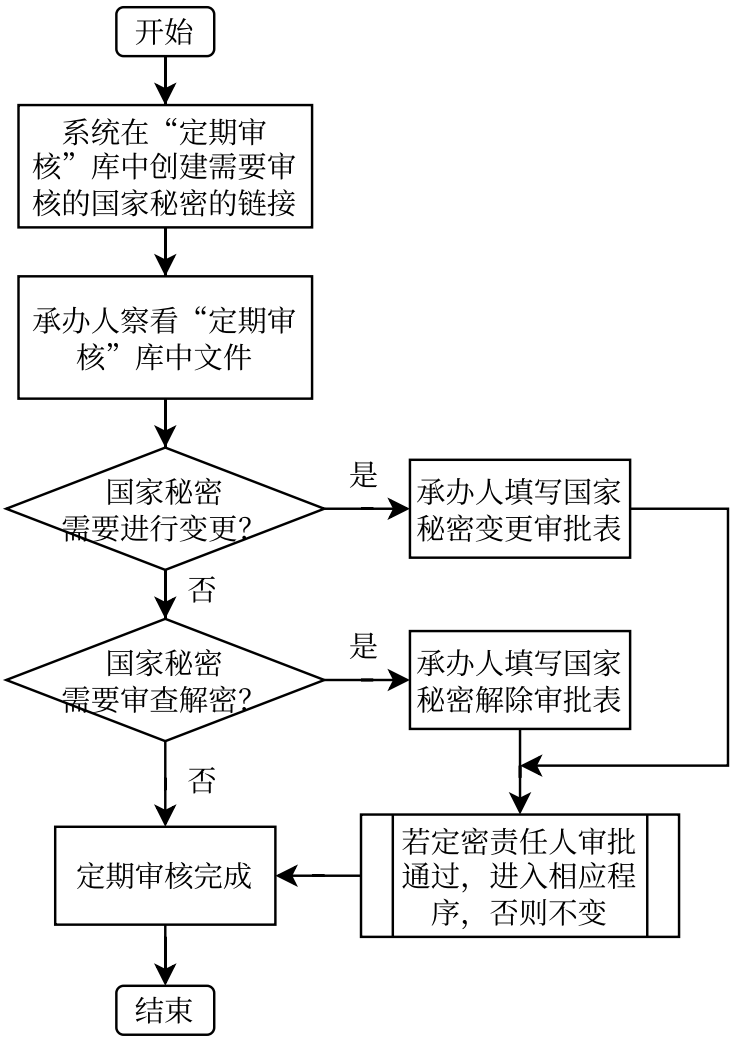
1. 在定密授权中的流程


开始
主动授权
依申请授权
授权机关选定被授权机关、单位
授权机关选定定密事项
系统分析并对此次授权是否合适作出建议
否
授权机关参考建议后继续授权?
是
系统检测被授权机关“经常产生国家秘密”?
否
是
系统自动查找最合适的授权机关
被授权机关在系统中补充定密授权申请审批表，系统自动补充附件
授权机关审批通过?
否
是
主动授权中止
授权完成，系统告知授权主体与客体
申请授权被拒绝
结束

2. 在国家秘密确定中的流程



3. 在国家定期审核中的流程



四、 总结

展望当下，计算机技术日新月异；放眼未来，定密工作将因定密工作管理系统如虎添翼。虽然鉴于对保密技术的认知不足、以及自身仍在计算机安全的技术学习中，此次定密工作管理系统并没有得到代码层面的实现，但这并不意味着这款系统仅仅是空中楼阁。它是《定密理论与实务》课程知识汇聚而成的结晶，是本学期学习的见证，更希望有朝一日这套系统能够真正得到实现，助力定密工作技术的发展。

参考文献

[1] 霍然. 浙江: 先行先试定密信息管理系统[J]. 保密工作, 2012: 34-35.

[2] 吴国华, 霍晨晨. 一种根据文档相似度快速查找定密依据的方法[J]. 保密科学技术, 2014: 12-15.

[3] 刘名, 毕颖. 论我国定密权专职化制度的建立[J]. 湖南社会科学, 2011: 98-100.

[4] 李先哲. 基于机器学习的数字化定密技术研究[D]. 天津大学, 2018.

[5] 王利培. 基于工作流的保密信息管理系统的设计与实现[D]. 西安电子科技大学, 2020.