ХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ
РИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ
12.2019.T.07.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ
ЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

АЛАЕВ РУҲИЛЛО ҲАБИБОВИЧ

АХБОРОТНИНГ КРИПТОГРАФИК МУҲОФАЗАСИ УЧУН МОДЕЛ, АЛГОРИТМ ВА ДАСТУРЛАР

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги.

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент - 2022

УДК: 004.056

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора (PhD) по техническим наукам

Contents of dissertation abstract of doctor of philosophy (PhD) on technical sciences

Алаев Руҳилло Ҳабибович
Ахборотнинг криптографик муҳофазаси учун модел, алгоритм ва дастурлар.....3

Алаев Рухилло Хабибович

защиты
.....21

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

АЛАЕВ РУҲИЛЛО ҲАБИБОВИЧ

АХБОРОТНИНГ КРИПТОГРАФИК МУҲОФАЗАСИ УЧУН МОДЕЛ, АЛГОРИТМ ВА ДАСТУРЛАР

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги.

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент - 2022

Техника фанлари бўйича фалсафа доктори (Doctor of Philosophy) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида №B2019.2.PhD/FM388 рақам билан рўйхатга олинган.

Диссертация Мирзо Улуғбек номидаги Ўзбекистон Миллий Университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида (www.tuit.uz) ва «ZiyoNet» Ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий раҳбар:	**Арипов Мерсаид Мирсиддикович** физика-математика фанлари доктори, профессор
Расмий оппонентлар:	**Керимов Комил Фикратович** техника фанлари доктори, доцент
	Саттаров Алижон Бозорбоевич физика-математика фанлари бўйича фалсафа доктори (PhD)
Етакчи ташкилот:	**"UNICON.UZ" ДУК – Фан-техника ва маркетинг тадқиқотлари маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.02 рақамли Илмий кенгашнинг 2022 йил «17» август да соат 12⁰⁰ даги мажлисида бўлиб ўтади. (Манзил: 100084, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университетининг Ахборот-ресурс марказида танишиш мумкин (2700 рақам билан рўйхатга олинган). Манзил: 100084, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43).

Диссертация автореферати 2022 йил «17» август куни тарқатилди.
(2022 йил «17» августдаги 6 рақамли реестр баённомаси).

Б.Ш. Махкамов
Илмий даражалар берувчи илмий кенгаш раиси, иқтисод фанлари доктори, профессор

Э.Ш. Назирова
Илмий даражалар берувчи илмий кенгаш илмий котиби, техника фанлари доктори, доцент.

С.К. Ганиев
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, техника фанлари доктори, профессор

КИРИШ (фалсафа доктори (PhD) диссертацияси аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳонда ахборот хавфсизлигини таъминлаш учун янги усул, алгоритм, восита ва тизимларни ишлаб чиқиш ҳамда мавжудларини таҳлил қилиш ва такомиллаштиришга катта эътибор қаратилмоқда. Ахборотнинг криптографик муҳофазасини таъминлаш учун миллий криптографик алгоритмларни қўллаб-қувватлайдиган криптопровайдерлардан фойдаланиш муҳим аҳамият касб этади. Ушбу криптопровайдерлар Windows операцион тизимларидаги драйверлар ва амалий дастурлар учун маълумотларни шифрлаш, хэшлаш, имзолаш, имзосини текшириш, калитларни генерация қилиш, сақлаш, экспорт ва импорт қилиш, муомаладан чиқариш ва бошқа бир қатор криптографик амалларни бажаришни таъминлайди. Шу сабабли, кўплаб мамлакатларда, жумладан АҚШ, Россия, Хитой, Буюк Британия, Ҳиндистон, Жанубий Корея, Белоруссия, Украина, Қозоғистон, Ўзбекистон ва бошқа давлатларда криптопровайдер дастурий воситаларини яратиш ва таҳлил қилиш бўйича фаол илмий тадқиқотлар олиб борилмоқда.

Жаҳонда ахборот тизимлари ҳамда улардаги ахборотнинг хавфсизлигини таъминлаш усуллари, алгоритмлари ва тизимларини ишлаб чиқишга йўналтирилган илмий тадқиқотлар олиб борилмоқда. Ушбу тадқиқотлар ахборотнинг криптографик муҳофазаси учун мавжуд усул ва алгоритмлари тадқиқ қилиш ҳамда стандартларга жавоб берадиган криптографик модулларни яратиш, криптографик модулларга қаратилган таҳдидларни тадқиқ қилишга йўналтирилган. Шунга қарамай йилдан-йилга ортиб бораётган кибертаҳдидлардан ахборотнинг ҳимоясини таъминлаш учун янги алгоритм, усул ва воситаларни ишлаб чиқиш ва такомиллаштириш муҳим вазифалардан ҳисобланади.

Республикамизда ҳам ахборот тизимларини кибертаҳдидлардан ҳимоялаш ва ундаги маълумотларнинг бутунлиги, конфиденциаллиги ҳамда фойдаланувчанлигини таъминлашга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан: «... ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоя қилиш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга ўз вақтида ва муносиб қаршилик кўрсатиш...»[1] вазифалари белгиланган. Мазкур вазифаларни амалга оширишда миллий криптографик алгоритмларни қўллаб-қувватлайдиган криптопровайдерни яратиш ва криптографик калитларни самарали бошқаришни таъминлаш заруратини белгилайди.

Ушбу диссертация тадқиқоти Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисидаги»ги Фармони, 2018 йил 21 ноябрдаги ПҚ-4024-сон “Ахборот технологиялари ва

[1] Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги Фармони.

коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чора тадбирлари тўғрисида"ги Қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга ушбу тадқиқот иши муайян даражада хизмат қилади.

Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги. Диссертация республика фан ва технологиялар ривожланишининг IV. «Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

Муаммонинг ўрганилганлик даражаси. Ахборотнинг криптографик муҳофазаси учун моделлар, алгоритмлар ва воситаларини ишлаб чиқиш бўйича дунё бўйлаб бир қатор олимлар томонидан тадқиқотлар олиб борилган. Windows операцион тизимидаги CNG (Cryptography API: Next Generation) криптопровайдерларни ва уларнинг қўллаб-қувватлайдиган алгоритмларини таҳлили бўйича Y. Ahmad[1] тадқиқот олиб борган. Windows операцион тизимидаги калитларни сақлаш CNG криптопровайдерларининг архитектурасини ҳамда ушбу турдаги криптопровайдерларни яратиш устида Z. Lina[2] тадқиқот олиб борган. K. Lee, H. Lee, Y. Lee, K. Yim, J. Park, I. You, I. Oh, S. Lee олимлар CNG кутубхоналарининг калитларни сақлаш механизмини таҳлили[3], CNG кутубхоналари хавфсизлигини таҳлили[4], CNG кутубхоналарига таҳдидлар, CNG криптографик кутубхонасида SSL (Secure Sockets Layer) коммуникация жараёнларининг таҳлили, CNG интерфейси хоссалари, структураларини таҳлили бўйича тадқиқотлар олиб боришган. Ахборотнинг криптографик муҳофазаси учун "Microsoft Primitive Provider", "Microsoft Software Key Storage Provider", "Microsoft SSL Protocol Provider", "Microsoft Smart Card Key Storage Provider" номли CNG криптопровайдерлари (Microsoft, АҚШ), "ViPNet CSP" (ИнфоТеКС, Россия), "КриптоПро CSP" (КриптоПро, Россия), "Signal-COM CSP" (Сигнал-КОМ, Россия), "Валидата CSP" (Валидата, Россия), "Лисси CSP" (ЛИССИ-Софт, Россия), "Tumar CSP" (Гамма Технологиялар, Қозоғистон), "AVEST CSP" (АВЕСТ, Белоруссия), "IIT" (IIT, Украина) криптопровайдерлари яратилган.

Республикамизда ахборот хавфсизлигини таъминлашнинг интеллектуал тизимларини яратиш, ахборот хавфсизлигини таъминлашнинг усул ва воситаларини яратиш, тасодифий сонларни генерациялаш, симметрик шифрлаш, хэш-функция ва электрон рақамли имзо алгоритмларини яратиш ҳамда компьютер тизимларида фойдаланишни чеклашнинг концептуал

---

[1] Y. Ahmad. "A study on algorithms supported by CNG of Windows Operating System". // International Journal of Modern Engineering Research (IJMER). 2012, Vol.2, Issue.1, pp. 276-280.

[2] Z. Lina. "Design and Implementation of KSP on the Next Generation Cryptography API". // International Conference on Medical Physics and Biomedical Engineering (ICMPBE), vol. 33, pp. 1640-1646, Sep. 2012.

[3] K. Lee, H. Lee, Y. Lee and K. Yim, "Analysis on the Key Storage Mechanism of the CNG Library" // 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, 2016, -pp. 499-502.

[4] K. Lee, I. Oh, S. Lee, K. Yim. Vulnerability Analysis on the CNG Crypto Library. // The Journal of Korean Institute of Communications and Information Sciences. Vol.42 No.04, -pp. 838-847.

моделини ишлаб чиқиш бўйича Т.Ф.Бекмуродов[1], М.М.Арипов, С.К.Ганиев[2], Р.Ҳ.Ҳамдамов[3], Р.Д.Алоев[4], М.М.Каримов[5], П.Ф.Хасанов, А.В.Кабулов[6], Б.Ф.Абдурахимов[7], Г.У.Жураев[8], Д.Я.Иргашева[9] бошчилигидаги илмий жамоалар томонидан тадқиқотлар олиб борилган.

"O'zDSt 1106:2009 – хэшлаш функциялари", "O'zDSt 1105:2009 – маълумотларни шифрлаш алгоритми", "O'zDSt 1092:2009 – электрон рақамли имзони шакллантириш ва текшириш жараёнлари" стандартларининг алгоритмларни қўллаб-қувватлайдиган криптопровайдерларни яратиш, криптографик алгоритмларни операцион тизимда татбиқ этиш усуллари бўйича ҳозирги кунда етарли даражада илмий изланишлар олиб борилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги.

Диссертация тадқиқоти Мирзо Улуғбек номидаги Ўзбекистон Миллий университети ОТ-2018-Атех-546 «Android ва IOS операцион тизимлар учун мобил иловалар яратиш» (2018-2020) мавзудаги лойиҳа доирасида бажарилган.

Тадқиқотнинг мақсади ахборотнинг криптографик муҳофазасини таъминлаш учун "O'zDSt 1106:2009 – хэшлаш функцияси", "O'zDSt 1105:2009 – маълумотларни шифрлаш алгоритми" ва "O'zDSt 1092:2009 – электрон рақамли имзони шакллантириш ва текшириш жараёнлари" стандартларининг алгоритмларини қўллаб-қувватлайдиган криптопровайдерни яратиш ва криптографик калитларни самарали бошқаришни таъминлашдан иборат.

Тадқиқотнинг вазифалари:

O'zDSt 1092:2009 стандартидаги биринчи алгоритмнинг калитлари ёрдамида умумий махфий калитни генерациялаш алгоритмини яратиш;

O'zDSt 1092:2009 алгоритмининг калитларига рухсатларни бошқариш алгоритмини яратиш;

---

[1] Bekmuratov T.F., Botirov F.B. Development of structures of intellectual information protection system, Chemical technology. control and management. 2019. vol. 6, No. 90, -pp. 63-71.

[2] Ganiyev S.K., Khudoykulov Z.T., Halimtaeva I.U., Computer's source based (Pseudo) random number generation. //2017 Information Science and Communications Technologies (ICISCT), Tashkent 2017, –pp. 1-6.

[3] Askar T. Rakhmanov, Rustam Kh. Khamdamov, Komil F. Kerimov, Shukhrat K. Kamalov, Automatic Vulnerability Detection Algorithm for the SQL-Injection. // Journal of Automation and Information Sciences. 2019. Vol. 51, Issue 7. -pp. 47-54.

[4] Aloev R.D., Nurullaev M. Software, algorithms and methods of data encryption based on national standards. // IIUM Engineering Journal. 2020, Vol. 21, issue 1, -pp. 142-166.

[5] Kodirov Z.Z., Karimov M.M., Tashev K.A., Gulomov Sh.R., Islomova M.X. Artificial Intelligence, Ensuring Information Security In Virtual Robots And Extensive Use Of Smart Systems. // American Journal of Engineering and Technology. 2020. Vol 2 No 08. -pp. 28-38.

[6] Кабулов А.В., Варисов А.А., Каландаров И. Оценка рисков информационной безопасности и обеспечение конфиденциальности информационных ресурсов. // Проблемы информатики и энергетики. 2017. — №6.— С.27-36.

[7] Abdurakhimov B.F., Sattarov A.B. An algorithm for constructing S-boxes for block symmetric encryption // International Journal: "Universal Journal of Mathematics and Applications". 2018. Vol.1, No.1 -pp. 29-32.

[8] Juraev G.U., Ikramov A.A., Marakhimov A.R. About differential cryptanalysis algorithm of block encryption "Kuznyechik". // International Journal of Advanced Research in Science, Engineering and Technology. 2019. Vol. 6, Issue 2. -pp. 8164-8169.

[9] Irgasheva D., Khurramov D., Rustamova S., Approaches to Formalizing the Access Control System. // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent 2021, –pp. 1-4.

O‘zDSt 1092:2009 алгоритми калитларининг хавфсиз сақланишини таъминлаш усулини яратиш;

криптопровайдерлар учун таҳдидларни таҳлил қилиш, таҳдид моделини ишлаб чиқиш ва баҳолаш;

O‘zDSt 1105:2009, O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмларини қўллаб-қувватлайдиган криптопровайдерни яратиш;

O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмлари асосида яратилган рақамли сертификатларнинг Windows операцион тизими томонидан танилишини таъминлайдиган криптографик модулни яратиш.

Тадқиқотнинг объекти сифатида Windows операцион тизимларида криптографик амалларни бажарадиган криптопровайдерлар олинган.

Тадқиқотнинг предметини ахборотнинг криптографик муҳофазасини таъминлаш учун “O‘zDSt 1106:2009 – хэшлаш функцияси”, “O‘zDSt 1105:2009 – маълумотларни шифрлаш алгоритми”, “O‘zDSt 1092:2009 – электрон рақамли имзони шакллантириш ва текшириш жараёнлари” стандартларининг алгоритмларни қўллаб-қувватловчи криптопровайдерни яратиш ва криптографик калитларни бошқариш усуллари ташкил этади.

Тадқиқотнинг усуллари. Тадқиқот жараёнида ахборотни криптографик ҳимоялаш усуллари, сонлар назарияси, моделлаштириш, тизимли дастурлаш ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

O‘zDSt 1092:2009 стандартидаги биринчи алгоритмнинг калитлари асосида симметрик криптотизимлар учун умумий махфий калитни генерациялаш алгоритми яратилган;

хэшлаш функцияси асосида компьютердаги турли имтиёзга эга фойдаланувчилар калитларининг хавфсизлигини оширувчи усул яратилган;

веб сервис технологияси асосида мобил қурилмадаги электрон рақамли имзо калитларига рухсатларни самарали бошқариш алгоритми яратилган;

STRIDE услубияти асосида криптопровайдерлар учун таҳдид модели ишлаб чиқилган, шунингдек ахборот хавфсизлиги таҳдидлари таснифланган ва DREAD услубияти асосида баҳоланган;

Windows операцион тизимининг стандарт криптографик интерфейсларини қўллаган ҳолда O‘zDSt 1105:2009, O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 миллий стандартлардаги алгоритмлар орқали ахборотнинг конфиденциаллиги ва бутунлигини бузишга қаратилган кибертаҳдидлардан ҳимоялашни таъминлайдиган “Хэш, имзо ва симметрик шифрлаш криптопровайдери” дастурий воситаси ишлаб чиқилган;

Windows операцион тизимининг Active Directory сертификатлаш хизмати билан интеграция қилиш орқали O‘zDSt 1092:2009 стандартидаги алгоритмларнинг калитларини самарали бошқаришни таъминлайдиган “Калитларни сақлаш криптопровайдери” дастурий воситаси яратилган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

Microsoft Office иловаларида ҳужжатларнинг хавфсизлигини таъминлаш учун миллий криптографик алгоритмлардан фойдаланиш имкони яратилган;

O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмлари асосида яратилган рақамли сертификатларнинг Windows операцион тизими томонидан танилишини таъминлаш модули яратилган;

Active Directory сертификатлаш хизмати орқали O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмларини қўллаб-қувватлайдиган “Очиқ калитлар инфратузилмаси” ни шакллантириш имконияти яратилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги яратилган криптопровайдерларнинг операцион тизим билан биргаликда ишлаши ва дастурий мажмуани амалга оширишда ишлаб чиқилган алгоритмлар бўйича ўтказилган тажрибаларнинг натижалари билан асосланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти таклиф этилган умумий махфий калитни генерациялаш алгоритми, криптопровайдерларни ишлаб чиқилганлиги, калитларга рухсатларни бошқариш ва калитларни хавфсиз сақлаш усуллари таклиф этилганлиги билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти ташкилотларда ахборотнинг криптографик муҳофазасини таъминлаш учун бир нечта ахборот тизимида ягона калитдан фойдаланиш, Windows операцион тизими томонидан O‘zDSt 1092:2009 алгоритми асосида яратилган рақамли сертификатларни қўллаб-қувватланиши, CNG интерфейсини қўллаб-қувватлайдиган криптопровайдерлардан фойдаланиш имкониятининг тақдим этилганлиги билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Диссертация тадқиқотлари доирасида ахборотнинг криптографик муҳофазасини таъминлаш учун олинган илмий натижалар асосида:

Электрон рақамли имзо калитларига рухсатларни бошқариш усули ва дастурий мажмуаси “UNICON.UZ” ДУК – Фан-техника ва маркетинг тадқиқотлари марказида “Ўзбекистон Республикаси очиқ калитлар инфратузилмасининг хавфсизлик сервисларини такомиллаштириш усуллари ва воситаларини ишлаб чиқиш” лойиҳасида фойдаланилди (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 30 ноябрдаги 33-8/8538 маълумотномаси). Илмий тадқиқот натижаларидан фойдаланиш маълумотларнинг конфиденциаллиги ва бутунлигини бузишга қаратилган таҳдидларни бартараф этишда криптографик усулларни қўллаш самарадорлигининг ошиши ҳамда ушбу дастурий таъминот республикамизда мавжуд калитларни рўйхатга олиш имконини берган;

Умумий калитни генерациялаш алгоритми, таҳдидлар модели ва дастурий таъминоти Муҳаммад Ал-Хоразмий номидаги Тошкент ахборот технологиялари университетида “БВ Ф4-023 – Тақсимланган ахборот тизимларида инцидентлар ва киберҳужумларга қарши ҳаракатларни бошқариш муаммоларини тадқиқ этиш” лойиҳасида жорий этилди

(Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 30 ноябрдаги 33-8/8538 маълумотномаси). Илмий тадқиқот натижаларидан фойдаланиш маълумотларнинг конфиденциаллиги ва бутунлигини бузишга қаратилган таҳдидларни бартараф этишда криптографик усулларни қўллаш самарадорлигини 10-12% ошириш имконини берган.

O'zDSt 1092:2009 ва O'zDSt 1106:2009 алгоритмлари асосида яратилган рақамли сертификатларни бошқариш ва ахборотнинг криптографик муҳофазасини таъминлаш дастурий таъминотлари "SMART SOFTWARE" МЧЖда "Қишлоқ қурилиш инвест иш жараёни автоматлашган ахборот тизими"да жорий этилди (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 30 ноябрдаги 33-8/8538 маълумотномаси). Илмий тадқиқот натижаларидан фойдаланиш маълумотларнинг конфиденциаллиги ва бутунлигини таъминлашда қўлланилиб, ахборот тизимида ахборотнинг криптографик муҳофазасини таъминлаш харажатларини икки бараварга камайтириш имконини берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 11 та, жумладан 5 та халқаро ва 6 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Тадқиқот мавзуси бўйича жами 20 та илмий иш чоп этилган, жумладан Ўзбекистон Республикаси Олий аттестация комиссиясининг докторлик диссертациялари асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларда 7 та мақола, шундан 2 таси хорижий ва 5 таси республика журналларида нашр этилган. Шунингдек, ЭҲМ учун яратилган 2 та дастурий воситаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан ташкил топган. Диссертациянинг ҳажми 120 бетдан иборат.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурати, тадқиқотнинг республика фан ва технологиялари ривожлантиришнинг устувор йўналишларига мос келиши асосланган. Диссертация мавзуси бўйича чет элдаги илмий тадқиқотларнинг қисқача маълумоти ва муаммонинг ўрганилганлик даражаси келтирилган, тадқиқотнинг мақсад, вазифалари шакллантирилган, унинг объекти ва предмети кўрсатилган, тадқиқотнинг амалий натижалари ва илмий янгиликлари баён қилинган, олинган натижаларнинг назарий ва амалий аҳамияти очиб берилган, тадқиқот натижаларининг қўлланилиши, диссертация тузилиши ва нашр қилинган илмий ишлар тўғрисида маълумотлар келтирилган.

Диссертациянинг **«Криптографик стандартлар, интерфейслар ва алгоритмларни операцион тизимларда татбиқ этиш муаммолари»** деб

номланган биринчи боби 3 та параграфдан иборат. Биринчи параграфда криптографик алгоритмларни операцион тизимда татбиқ этишнинг зарурати баён қилинган, жаҳондаги етакчи компаниялар томонидан яратилган криптопровайдерлар тадқиқ қилинган, уларнинг маълумотларни шифрлаш ва хэшлаш тезлиги таҳлил қилинган ва ишончлилиги баҳоланган. Иккинчи параграфда криптографик стандартлар таҳлил қилинган ва криптографик интерфейсларнинг қиёсий таҳлили келтирилган. Учинчи параграфда яратиладиган криптопровайдерларга талаблар ва криптографик алгоритмларни операцион тизимларда татбиқ этиш муаммолари баён қилинади.

Диссертациянинг **«Криптографик калитларни бошқаришнинг самарали усул ва алгоритмларини яратиш»** деб номланган иккинчи боби 3 та параграфдан иборат.

Иккинчи бобнинг §2.1 параграфида O‘zDSt 1092:2009 стандартидаги биринчи алгоритмнинг жуфт калитлари асосида умумий махфий калитни генерациялаш алгоритми ишлаб чиқилган. Алгоритмда қуйидаги белгилашлар киритилади:

(U_{az}, X_{az}) – А фойдаланувчи ёпиқ калити;
(Y_{ao}, Z_{ao}) – А фойдаланувчи очиқ калити;
(U_{bz}, X_{bz}) – В фойдаланувчи ёпиқ калити;
(Y_{bo}, Z_{bo}) – В фойдаланувчи очиқ калити;
K_a – А фойдаланувчи томонидан генерация қилинган махфий калити;
K_b – В фойдаланувчи томонидан генерация қилинган махфий калити;
L – генерация қилинадиган симметрик калитнинг битдаги узунлиги.

Алгоритмнинг асосий қадамлари:

1-қадам. А фойдаланувчи $K1$ ва $K2$ ни қуйидаги формулалар асосида ҳисоблайди:

$$K1 \equiv Y_{bo}^{\backslash U_{az}} (mod\ p).$$
$$K2 \equiv Z_{bo}^{\backslash X_{az}} (mod\ p).$$

2-қадам. $K = K1\ xor\ K2$.

3-қадам. $K_a \equiv K(mod\ 2^L)$.

4-қадам. В фойдаланувчи K1 ва K2 қийматларни қуйидаги формулалар асосида ҳисоблайди:

$$K1 \equiv Z_{ao}^{\backslash X_{bz}} (mod\ p).$$
$$K2 \equiv Y_{ao}^{\backslash U_{bz}} (mod\ p).$$

5-қадам. $K = K1\ xor\ K2$.

6-қадам. $K_b \equiv K(mod\ 2^L)$.

Бу ерда $K_a = K_b$ муносабат ўринли.

K_a ва K_b калитлар K_u билан белгилаб олинади. Бунда K_u – умумий махфий калит. Генерация қилинган K_u калит ёрдамида мавжуд K_s симметрик калитни шифрлаб узатиш мумкин, ёки K_u калитнинг хэш қийматини ҳисоблаб, K_s калит ўрнида фойдаланиш мумкин:

$$K_s = h(K_u),$$

бунда h – хэшлаш функцияси.

Таклиф этилган алгоритм O‘zDSt 1092:2009 стандартидаги биринчи алгоритмнинг калитларини нафақат электрон рақамли имзо учун балки симметрик шифрлашда симметрик калитларни узатиш учун ҳам қўллаш имконини беради.

Иккинчи бобнинг §2.2 параграфида STRIDE услубияти асосида криптопровайдерлар учун таҳдид модели ҳамда DREAD услубияти асосида таҳдидларни баҳолаш келтирилган. Таҳдидларни $t_i \in T, \quad i = \overline{1, N_t}$, ҳимояланиши керак бўлган ресурсларни $m_j \in M, \quad j = \overline{1, N_m}$ ҳамда таҳдидлардан ҳимоя чораларини $h_k \in H, \; k = \overline{1, N_h}$ билан белгилаб олинади. Ҳар бир таҳдидни 5 та атрибут $(D_i; R_i; E_i; A_i; Di_i)$ орқали ифодалаймиз. Бунда $D_i, R_i, E_i, A_i, Di_i \in \{1; 2; 3\}$ ҳар бир таҳдиднинг DREAD услубияти бўйича баҳоларини ифодалайди. Таҳдиднинг 5 та атрибути асосида таҳдидларнинг хавфлилик даражаси $X(t_i)$ қуйидаги формула асосида ҳисобланади:

$$X(t_i) = (D_i + R_i + E_i + A_i + Di_i).$$

i-таҳдид рейтинги $TR(t_i) \in$ {юқори, ўрта, қуйи} қуйидаги формула орқали ҳисобланади:

$$TR(t_i) = \begin{cases} \text{юқори}, & \text{агар } 12 \le X_i \le 15 \\ \text{ўрта}, & \text{агар } 8 \le X_i \le 11 \\ \text{қуйи}, & \text{агар } 5 \le X_i \le 7. \end{cases}$$

i-таҳдиднинг $TN(t_i)$ – нисбий муҳимлик даражасини аниқлаш учун қуйидаги формуладан фойдаланилади:

$$TN(t_i) = \frac{X(t_i)}{\sum_{j=1}^{N_t} X(t_j)},$$

$$\sum_{i=1}^{N_t} TN(t_i) = 1.$$

Таҳдидлар, ресурслар ва ҳимоя чоралари ўртасидаги муносабатни граф кўринишида ифодалаш мумкин:

$$G(V, E) = \langle V, E \rangle, V = T \cup M \cup H, T \neq \emptyset, M \neq \emptyset, H \neq \emptyset,$$
$$E \subseteq T \times M \cup T \times H \cup M \times H$$

Бунда граф учлари 3 хил турда бўлиб, таҳдидлар, ресурслар ва ҳимоя чораларини ифодалайди. (t_i, m_j) граф қирраси m_j ресурс учун t_i таҳдид мавжудлигини, h_k ҳимоя чораси m_j ресурсни t_i таҳдиддан ҳимоясини таъминлашини (t_i, m_j, h_k) вектор ифодалайди.

Ресурс учун таҳдидларни ифодаловчи $\omega(t_i, m_j)$ функцияни аниқлаймиз:

$$\omega(t_i, m_j) = \begin{cases} 1, \text{агар } m_j \text{ ресурсга } t_i \text{ таҳдид мавжуд бўлса}, \\ 0, \quad \text{акс ҳолда}. \end{cases}$$

$f(t_i, m_j)$: $E' \times H \to [0,1]$ акслантириши агар m_j ресурс учун t_i таҳдиддан ҳимоясини таъминловчи ҳеч бўлмаганда битта h_k ҳимоя чораси мавжуд бўлса, у ҳолда $f(t_i, m_j) = 0$, акс ҳолда $f(t_i, m_j) = 1$ ни ифодалайди.

Ҳар бир m_j ресурс учун $rb(m_j)$ риск баҳоси қуйидаги формула орқали ҳисобланади, бунда қуйи рейтингга эга таҳдидлар инобатга олинмайди:

$$rb(m_j) = \sum_{i=1}^{N_t} \begin{cases} 0, \text{агар } TR(t_i) = \text{қуйи}, \\ \omega(t_i, m_j) * TN(t_i), \text{акс ҳолда}. \end{cases}$$

Барча ресурслар учун ёки тизим даражасида RB риск баҳоси қуйидаги формула билан ҳисобланади:

$$RB = \sum_{j=1}^{N_m} rb(m_j).$$

Ҳар бир m_j ресурс учун $rbh(m_j)$ ҳимоя чоралари қўлланилгандан кейинги риск баҳоси қуйидаги формула орқали ҳисобланади, бунда қуйи рейтингга эга таҳдидлар инобатга олинмайди:

$$rbh(m_j) = \sum_{i=1}^{N_t} \begin{cases} 0, \text{агар } TR(t_i) = \text{қуйи}, \\ f(t_i, m_j) * rb(m_j), \quad \text{акс ҳолда}. \end{cases}$$

Ҳимоя чоралари қўлланилгандан кейин барча ресурслар учун ёки тизим даражасида RBH риск баҳоси қуйидаги формула асосида ҳисобланади:

$$RBH = \sum_{j=1}^{N_m} rbh(m_j).$$

Ҳимоя чоралари қўлланилганда эришиладиган самарадорлик кўрсаткичини қуйидаги формула асосида ҳисобланади:

$$SK = \frac{RB - RBH}{RB}.$$

Иккинчи бобнинг §2.3 параграфида криптографик калитга рухсатларни бошқариш алгоритми баён қилинган. Мобил қурилмалардаги калитларга мурожаат қилиш учун таклиф этилаётган тизим архитектураси 3 та модулдан иборат: амалий дастурлардан сўровларни қабул қилувчи криптографик модул – C_c, мобил қурилмадаги криптографик модул – C_m ва веб сервис – W. Қуйидаги белгилашларни киритамиз:

E – асимметрик шифрлаш алгоритмининг шифрлаш функцияси;

E' – симметрик шифрлаш алгоритмининг шифрлаш функцияси;

D – асимметрик шифрлаш алгоритмининг расшифровкалаш функцияси;

D' – симметрик шифрлаш алгоритмининг расшифровкалаш функцияси;

$h(x)$ – хэшлаш функцияси;

M – имзолаш учун маълумотлар;

H – хэш қиймат;

K_{ou} – фойдаланувчи очиқ калити;

K_{pu} – фойдаланувчи ёпиқ калити;

K_{ow} – веб сервис W очиқ калити;

K_{pw} – веб сервис W ёпиқ калити;

K_{ms} ва K_{cs} – симметрик калитлар;

L_f – фойдаланувчининг W – сервисдаги логини, логин телефон номери, почта адреси бўлиши мумкин;

App – амалий дастур;

W – веб сервис, C_c ва C_m криптографик модуллар ўртасида алоқани таъминлаш учун хизмат қилади. Бу ерда фойдаланувчининг сертификатлари, логини ва вақтинчалик пароли сақланади. Ҳар бир фойдаланувчининг бир нечта сертификати бўлиши мумкин.

Ҳар бир фойдаланувчи олдин тизимда рўйхатдан ўтади. Қуйидаги жараёнлар модулларнинг ўзаро алоқасини қадамба-қадам намойиш этади.

Рўйхатдан ўтиш жараёни. Рўйхатдан ўтиш жараёни C_m ва W веб сервис орқали амалга оширилади. У қуйидаги қадамларни ўз ичига олади:

1-қадам. C_m томонда фойдаланувчи {янги жуфт калитни генерация қилиш, мавжуд жуфт калитни импорт қилиш} амалларидан бирини танлайди.

2-қадам. Фойдаланувчи C_m томонда ПИН-кодни киритади.

3-қадам. Агар фойдаланувчи мавжуд жуфт калитни импорт қилишни танлаган бўлса, 7-қадамга ўтилади, акс ҳолда 4-қадамга ўтилади.

4-қадам. C_m томон янги $\{K_{pu}, K_{ou}\}$ жуфт калитни генерация қилади. C_m томон ёпиқ калитни шифрлайди, $\{K'_{pu}, K_{ou}, H_k\}$ қийматларни доимий хотирада сақлайди.

5-қадам. C_m томон фойдаланувчидан идентификация маълумотларни сўраб олиб, рақамли сертификат олиш учун сўров (*CSR(certificate signing request)*) ни генерация қилади ва CSRни *Регистрация марказига (RA)* юборади.

6-қадам. C_m томон *RA* томондан олинган рақамли сертификатни импорт қилади, 9-қадамга ўтилади.

7-қадам. C_m томон фойдаланувчидан паролни сўраб олиб, *PKCS#12* форматдаги жуфт калитларни импорт қилади.

8-қадам. C_m томон K_{pu} ни шифрлайди, $\{K'_{pu}, K_{ou}, H_k$, сертификат$\}$ қийматларни доимий хотирада сақлайди.

9-қадам. C_m томон фойдаланувчидан L_f логинни сўраб олади, $H = h(L_f)$, $S = E_{K_{pu}}(H)$ ҳисоблайди ва $\{L_f$, S, фойдаланувчи сертификати$\}$ маълумотларни W томонга узатади.

10-қадам. W томон агар $D_{K_{ou}}(S) = h(L_f)$ бўлса, 11-қадамга ўтади, акс ҳолда "Incorrect params" хатолик билан жавоб қайтаради.

11-қадам. Агар L_f бошқа фойдаланувчи томонидан банд қилинмаган бўлса, унда 16-қадамга ўтади.

12-қадам. W томон «W да мавжуд бўлган ҳамда L_f томонга олдин бириктирилган рақамли сертификатлар жорий фойдаланувчига тегишлигини» текширади. Бу учун W томон L_f томонга олдин бириктирилган рақамли сертификатларни олади, T тасодифий сонни генерация қилади, $T' = E_{K_{ou}}(T)$, $S = E_{K_{pw}}(h(T'))$ қийматларни ҳисоблайди ва $\{T', S$, сертификатлар рўйхати$\}$ – қийматларни C_m томонга узатади.

13-қадам. C_m томон W томондан узатилган сертификатлар ичида унга тегишли сертификат бўлмаса, 14-қадамга ўтади, акс ҳолда C_m ўзига тегишли сертификатни танлаб олиб, агар $h(T') = D_{K_{ow}}(S)$ бўлса, $T = D_{K_{pu}}(T')$, $T' = E_{K_{ow}}(T)$, $S = E_{K''_{pu}}(h(T'))$ ҳисоблаб, $\{T', S, C_m$ томон танлаган сертификат$\}$ ни W томонга узатади, 15-қадамга ўтилади. Бунда K''_{pu} қиймат – C_m томон танлаган сертификатнинг ёпиқ калити.

14-қадам. C_m "Логин банд" лиги ҳақида фойдаланувчига хабар беради. 9-қадамга ўтилади.

15-қадам. W агар $h(T') = D_{K_{ou}}(S)$ ва $T = D_{K_{pw}}(T')$ бўлса, 16-қадамга ўтилади, акс ҳолда "Incorrect params" хатолик билан жавоб қайтаради.

16-қадам. W томон фойдаланувчини рўйхатдан ўтказади, L_f ва сертификатни маълумотлар базасида сақлайди, «Successful» мазмундаги рўйхатдан ўтиш муваффақиятли тугаганлигини билдирувчи жавоб хабар узатади.

17-қадам. C_m томон фойдаланувчига рўйхатдан ўтиш муваффақиятли тугаганлигини билдирувчи хабарни кўрсатади ва W томон билан алоқани узади.

Имзони шакллантириш жараёни. Имзолаш жараёнида 3 та модул қатнашади. Ушбу жараён қуйидаги қадамларни ўз ичига олади:

1-қадам. *App* томон C_c билан маълумотни имзолаш учун алоқани ўрнатади.

2-қадам. C_c томон фойдаланувчидан L_f логинни сўраб олади.

3-қадам. C_c бир марталик P паролни генерация қилади ва уни фойдаланувчига *QR-код* кўринишида тақдим этади.

4-қадам. C_m томон *QR-код*ни сканер қилиб, P-ни ўқиб олади. C_m фойдаланувчида биттадан кўп сертификат бўлса, C_m томон фойдаланувчидан имзолаш учун қайси сертификатдан фойдаланишини сўраб олади, акс ҳолда мавжуд ягона сертификатни олади.

5-қадам. C_m ёпиқ калитга мурожаат қилиш учун фойдаланувчидан ПИН-кодни сўраб олади. $K = h(h(PINcode))$ ҳисоблайди, агар $H_k = h(K)$ бўлса, унда $K_{pu} = D'_K(K'_{pu})$, акс ҳолда "ПИН-код хато" мазмунли хабар фойдаланувчига кўрсатилади ва 5-қадамга ўтилади.

6-қадам. C_m томон $K_s = h(h(P)), H = h(K_s), H' = E_{K_{ow}}(H), K'_s = E_{K_{pu}}(h(H'))$ ҳисоблайди.

7-қадам. C_m томон $\{L_f$, имзолаш учун қўлланиладиган фойдаланувчи сертификати$\}$- қийматларни W томонга узатади.

8-қадам. W сервис T тасодифий сонни генерация қилади, $T' = E_{K_{ou}}(T)$, $S = E_{K_{pw}}(h(T'))$ ҳисоблайди, $\{T', S\}$ қийматларни C_m томонга узатади.

9-қадам. C_m агар $h(T') = D_{K_{ow}}(S)$ бўлса, $T = D_{K_{pu}}(T')$, $T'' = E_{K_{ow}}(T)$, $S = E_{K_{pu}}(h(T''))$ ҳисоблаб, $\{L_f, T'', S, H', K'_s\}$ қийматларни W томонга узатади. H' ва K'_s қийматлари 6-қадамда ҳисобланган.

10-қадам. W томон, агар $h(T'') = D_{K_{ou}}(S)$ ва $T = D_{K_{pw}}(T'')$ ва $h(H') = D_{K_{ou}}(K'_s)$ бўлса, $P' = D_{K_{pw}}(H')$ ҳисоблайди, W томон L_f учун бир марталик P' паролни ўрнатади.

11-қадам. C_c томон $K_s = h(h(P)), H = h(K_s), H' = E_{K_{ow}}(H)$ ҳисоблайди ва $\{L_f, H'\}$ қийматларни W томонга аутентификациядан ўтиш учун узатади.

12-қадам. W сервис $P' = D_{K_{pw}}(H')$ ҳисоблайди, агар L_f ва P' тўғри бўлса, W томон C_c томонга имзолаш учун қўлланиладиган сертификатни қайтаради, акс ҳолда "Incorrect login and/or password" мазмунли хабар жўнатади.

13-қадам. C_c агар W томондан "Incorrect login and/or password" мазмунли хабар олса, хабарни фойдаланувчига кўрсатади. 2-қадамга ўтади.

14-қадам. C_c томон фойдаланувчи сертификатини *App* томонга узатади.

15-қадам. *App* томон фойдаланувчи сертификати ва *M*-маълумотни хэшлаш учун C_c томонга узатади.
16-қадам. C_c томон $H = h(M)$ ҳисоблайди ва уни *App* томонга қайтаради. Хэш алгоритм сертификат асосида аниқланади.
17-қадам. *App* томон *H*-ни C_c томонга имзолаш учун узатади.
18-қадам. C_c томон $H'_c = E'_{K_s}(H)$ ҳисоблайди, {H'_c, фойдаланувчи сертификати}-ни W томонга узатади. C_c томон учун K_s 11-қадамда ҳисобланган.
19-қадам. W томон {H'_c, фойдаланувчи сертификати}-ни C_m томонга узатади.
20-қадам. C_m томон {H'_c, фойдаланувчи сертификати}-ни W томондан олади.
21-қадам. C_m томон фойдаланувчидан имзолашга рухсат сўрайди.
22-қадам. Агар фойдаланувчи рухсат берса, C_m томон $H = D'_{K_s}(H'_c)$, $S = E_{K_{pu}}(H)$, $S' = E'_{K_s}(S)$ ҳисоблайди ва {S', "Successfully"}-қийматларни имзолаш натижаси сифатида W томонга узатади, акс ҳолда "Signature rejected" хабарни имзолаш натижаси сифатида W томонга узатади. C_m томон учун K_s 6-қадамда ҳисобланган.
23-қадам. W томон C_m томондан олган натижани C_c томонга узатади.
24-қадам. C_c агар имзолаш натижаси "Successfully" бўлса, $S = D'_{K_s}(S')$ ҳисоблайди ва {*S*, "Successfully"}-ни *App* томонга узатади, акс ҳолда "Signature rejected" хабарни *App* томонга узатади.
25-қадам. *App* агар имзолаш натижаси "Successfully" бўлса, *App* томон *S*-ни маълумот имзоси сифатида қўллайди.
26-қадам. *App* томон C_c томон билан алоқани узади.
27-қадам. C_c томон W томон билан алоқани узади.
28-қадам. W сервис P'-ни ўчиради.

Имзони текшириш жараёни. Имзони текшириш жараёни қуйидаги қадамлардан иборат:
1-қадам. *App* томон C_c томон билан имзони текшириш учун алоқани ўрнатади.
2-қадам. *App* томон C_c томонга имзо сертификатини ва M – маълумотни хэшлаш учун узатади.
3-қадам. C_c томон $H = h(M)$ ҳисоблайди, *H*-ни *App* томонга узатади.
4-қадам. *App* томон {*H*, *S*, имзо сертификати} ни C_c томонга узатади.
5-қадам. C_c агар $H = D_{K_{ou}}(S)$ бўлса, C_c "Signature is valid" хабарни, акс ҳолда "Signature is invalid" хабарни текшириш натижаси сифатида қайтаради.
6-қадам. *App* томон C_c томон билан алоқани узади.

Ушбу алгоритм мобил қурилмада жойлашган калитнинг ягона нусхасидан бошқа қурилмалардаги ахборот тизимларида ҳам фойдаланиш имкониятини тақдим этади.

Диссертациянинг **«Ахборотни криптографик муҳофазаси стандартларининг алгоритмларини қўллаб-қувватлайдиган криптопровайдерларни яратиш»** деб номланган учинчи бобида O'zDSt 1105:2009, O'zDSt 1106:2009 ва O'zDSt 1092:2009 стандартларининг алгоритмларини қўллаб-қувватлайдиган «ARH Primitive Provider» криптопровайдерни яратиш, O'zDSt 1092:2009 стандартидаги

алгоритмларнинг калитларини бошқариш учун калитларни сақлаш криптопровайдерини яратиш ҳамда O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмлари асосида яратилган рақамли сертификатларни қўллаб-қувватлаш модулини ишлаб чиқиш баён этилган.

Калитларни хавфсиз сақлаш усули. «ARH Key Storage Provider» криптопровайдерида калитларнинг хавфсизлигини таъминлашнинг ПИН-код асосида ва ПИН-кодсиз амалга ошириш имконияти яратилган. Агар ПИН-код кўрсатилган бўлса, калитни шифрлаш қуйидагича амалга оширилади:

$$Ke = Eu(Kp, Kb)$$

бунда Kp – шифрлаш калити, Kb – генерация қилинган ёпиқ калит, Eu – O‘zDSt 1105:2009 шифрлаш алгоритми.

Kp шифрлаш калити қуйидагича ҳисобланади.

$$Kp = h_u(h_u(h_u(PINcode)))$$

бунда h_u – O‘zDSt 1106:2009 хэшлаш функцияси.

Агар ПИН-код кўрсатилмаган бўлса, ёпиқ калитни шифрлаш *CryptProtectData* функцияси орқали амалга оширилади.

Калитлар жойлашган каталог ва калит сақланган файл учун “тизим (system)” ва “яширин (hidden)” атрибутлари ўрнатилади. Калитлар жойлашган каталогга ва калит файлига рухсат “тизим фойдаланувчиси (system account)”га ва “администраторлар” гуруҳига берилади. Агар бу фойдаланувчи даражасидаги калит бўлса, унда юқоридаги рухсатларга қўшимча равишда жорий фойдаланувчига ҳам берилади.

Рақамли сертификатлар билан ишлаш учун тизимда “*Криптопровайдер кенгайтмаси”* ишлаб чиқилган. Мазкур кенгайтма ўрнатилгандан сўнг операцион тизимнинг O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмлари асосида яратилган рақамли сертификатлар билан боғлиқ сўровларини қайта ишлайди, янги сертификатни чиқаришга сўровларни яратади, рақамли сертификат имзосини текшириш таъминлайди.

Диссертациянинг **«“ARH Primitive provider” ва “ARH Key storage provider” криптопровайдерлари дастурий воситаларининг татбиқи»** деб номланган тўртинчи бобида ахборотни ҳимоялашнинг миллий криптографик алгоритмларини қўллаб-қувватлайдиган «ARH Primitive Provider» ва «ARH Key Storage Provider» криптопровайдерларининг татбиқига бағишланган. Унда O‘zDSt 1092:2009 ва O‘zDSt 1106:2009 алгоритмларини қўллаб-қувватлайдиган “Очиқ калитлар инфратузилмаси”ни ишга тушириш, Microsoft Office иловаларида криптопровайдер билан интеграция қилинган ҳолда O‘zDSt 1105:2009 ва O‘zDSt 1106:2009 алгоритмларини қўллаб хавфсизлигини таъминлаш, яратилган криптопровайдерларни жорий этишдаги самарадорликни баҳолаш баён этилган ҳамда яратилган криптопровайдерлар ва бошқа криптографик модулларнинг қўллаб-қувватлайдиган функцияларнинг қиёсий таҳлили келтирилган (1-жадвал).

1-жадвал. Яратилган криптопровайдерлар ва бошқа криптографик модулларнинг қўллаб-қувватлайдиган функцияларнинг қиёсий таҳлили

№	Функция	ARH Primitive Provider, ARH Key Storage Provider (1-мавжуд, 0-мавжуд эмас)	Крипто-провай-дер бўлмаган крипто-график модуллар (1-мавжуд, 0-мавжуд эмас)	Фойда-ланиш коэффи-циенти (1-кам, 5-ўрта, 10-кўп)	A*K	B*K
		A	B	K		
1.	O‘zDSt 1092:2009 стандартидаги алгоритмларнинг жуфт калитларини яратиш, экспорт/импорт қилиш, қўллаш ва ўчириш.	1	1	10	10	10
2.	ПИН-код асосида аутентификациялаш.	1	1	10	10	10
3.	ПИН-кодсиз аутентификациялаш.	1	0	1	1	0
4.	Фойдаланувчи калитларини қўллаб-қувватлаш.	1	1	10	10	10
5.	O‘zDSt 1092:2009 стандартининг алгоритмлари билан имзони шакллантириш ва текшириш, O‘zDSt 1105:2009 ва ГОСТ 28147-89 стандартларининг алгоритмлари билан симметрик шифрлаш, O‘zDSt 1106:2009 стандартининг алгоритмлари билан маълумотларни хэшлаш.	1	1	10	10	10
6.	Операцион тизим сервис дастурлари учун криптографик амалларни тақдим этиш.	1	0	1	1	0
7.	Операцион тизимнинг O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмлари асосида яратилган рақамли	1	0	1	1	0

	сертификатлар билан ишлашини таъминлаш.					
8.	Microsoft Office иловаларида ҳужжатлар хавфсизлигини таъминлашда O‘zDSt 1106:2009 ва O‘zDSt 1105:2009 алгоритмларидан фойдаланиш.	1	0	1	1	0
9.	Калитларнинг хавфсизлигини таъминлашда операцион тизим ҳимоя усуллари (имтиёзларни бошқариш, калитлар жараёни изоляцияси, умумий калитларни шифрлаш) ни ва хусусий ҳимоя усулларини биргаликда интеграция қилинган ҳолда қўллаш.	1	0	1	1	0
10.	Симметрик шифрлаш алгоритмлари учун O‘zDSt 1092:2009 стандартидаги биринчи алгоритмнинг калитлари асосида умумий махфий калитни генерациялаш.	1	0	1	1	0
11.	Очиқ калитлар инфратузилмасини ташкил этиш.	1	1	10	10	10
12.	Очиқ калитлар инфратузилмасининг 2 поғонали иерархик моделини қўллаш.	1	1	10	10	10
13.	Очиқ калитлар инфратузилмасининг кўп поғонали иерархик моделини қўллаш.	1	0	1	1	0
14.	Турли мақсадлар учун рақамли сертификатларни яратиш, тузилмаси статик бўлмаган рақамли сертификатларни яратиш.	1	0	1	1	0
Жами					68	60

Яратилган криптопровайдерлар қўлланилганда ахборотнинг криптографик муҳофазасини таъминлашда Su – умумий самарадорлик қуйидагича ҳисобланади:

$$Su = \frac{\sum_{i=1}^{14} A_i * K_i - \sum_{i=1}^{14} B_i * K_i}{\sum_{i=1}^{14} A_i * K_i} * 100 = \frac{68 - 60}{68} * 100 \approx 12\%$$

ХУЛОСА

Диссертация иши ахборотнинг криптографик муҳофазаси учун модел, алгоритм ва дастурларни таҳлил қилиш ва яратишга бағишланган.

Тадқиқотнинг асосий натижалари қуйидагилардан иборат:

1. O‘zDSt 1092:2009 стандартидаги биринчи алгоритмнинг калитлари асосида умумий махфий калитни генерациялаш алгоритми яратилди, бу эса симметрик криптотизимларда O‘zDSt 1092:2009 алгоритми калитлари ёрдамида мавжуд симметрик калитларни шифрлаб узатиш имконини берди.

2. Калитларни хавфсиз сақлаш усули яратилди. Операцион тизим сервис дастурлари ва фойдаланувчи калитларини сақлаш учун алоҳида усул қўлланилди. Натижада сервис дастурларининг калитларини фақат сервис дастурларининг ўзи, бошқа фойдаланувчи калитларидан эса фақат аутентификациядан ўтган калитнинг эгаси фойдалана оладиган бўлди.

3. Криптопровайдерлар учун таҳдид модели STRIDE услубияти асосида ишлаб чиқилди. Криптопровайдер модулларига бўлиши мумкин бўлган таҳдидлар аниқланди ва таҳдидлар DREAD услубияти асосида баҳоланди. Таҳдидлар рейтингига қараб, самарали ҳимоя чораларини инобатга олган ҳолда дастурий таъминот ишлаб чиқилди.

4. Электрон рақамли имзо калитларига рухсатларни бошқариш алгоритми яратилди. Натижада калитнинг нусхаларини бир нечта қурилмаларда сақламасдан туриб, мобил қурилмадаги калитнинг ягона нусхасидан исталган сондаги ахборот тизимида фойдаланиш имкони яратилди.

5. O‘zDSt 1106:2009, O‘zDSt 1105:2009 ва O‘zDSt 1092:2009 алгоритмларини қўллаб-қувватлайдиган криптопровайдер ҳамда электрон рақамли имзо калитларнинг ҳаётийлик циклини бошқариш учун калитларни сақлаш криптопровайдери ишлаб чиқилди.

6. O‘zDSt 1106:2009 ва O‘zDSt 1092:2009 алгоритмлари асосида яратилган рақамли сертификатларни қўллаб-қувватлаш модули яратилди ҳамда Microsoft Office иловаларида O‘zDSt 1105:2009 ва O‘zDSt 1106:2009 алгоритмлари асосида ҳужжатларнинг хавфсизлиги таъминланди.

7. Яратилган криптопровайдерлар ахборот тизимларда ахборотнинг криптографик муҳофазасини таъминлаш харажатларини икки бараваргача камайтиради ҳамда операцион тизим билан интеграция қилинган ҳолда ишлаши натижасида маълумотларнинг конфиденциаллиги ва бутунлигини бузишга қаратилган таҳдидларни бартараф этишда криптографик модулларнинг тақдим этадиган функциялари ҳисобига криптографик усулларни қўллаш самарадорлигини 10-12% оширади.

НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.02 ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

АЛАЕВ РУХИЛЛО ХАБИБОВИЧ

МОДЕЛИ, АЛГОРИТМЫ И ПРОГРАММЫ ДЛЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ

Ташкент-2022

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за №B2019.2.PhD/FM388.

Диссертация выполнена в Национальном университете Узбекистана имени Мирзо Улугбека.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице Научного совета (http://tuit.uz) и на Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научный руководитель:	**Арипов Мерсаид Мирсиддикович** доктор физико-математических наук, профессор
Официальные оппоненты:	**Керимов Комил Фикратович** доктор технических наук, доцент
	Саттаров Алижон Бозорбоевич доктор философии (PhD) по физико-математическим наукам
Ведущая организация:	**ГУП «UNICON.UZ» Центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «27» августа 2022 г. в 12^{00} часов на заседании научного совета DSc.13/30.12.2019.T.07.02 при Ташкентском университете информационных технологий. (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №2700). (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «17» августа 2022 года.
(протокол рассылки №6 от «17» августа 2022 г.).

Б.Ш. Махкамов
Председатель научного совета по присуждению ученых степеней, доктор экономических наук, профессор

Э.Ш. Назирова
Ученый секретарь научного совета по присуждению ученых степеней, доктор технических наук, доцент

С.К. Ганиев
Председатель научного семинара при научном совете по присуждению ученых степеней, доктор технических наук, профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность диссертации. В мире особое внимание уделяется разработке новых методов, алгоритмов, средств и систем для обеспечения информационной безопасности, а также анализу и усовершенствованию существующих. Для обеспечения криптографической защиты информации важно использовать криптопровайдеров, поддерживающих национальные криптографические алгоритмы. Эти криптопровайдеры обеспечивают шифрование данных, хеширование, формированию подписи, проверку подписи, а также генерацию, хранению, экспорта и импорта, уничтожению ключей и ряд других криптографических операций для драйверов и приложений в операционных системах Windows. Поэтому во многих странах, в том числе в США, России, Китае, Великобритании, Индии, Южной Корее, Белоруссии, Украине, Казахстане, Узбекистане и других странах, ведутся активные научные исследования по созданию и анализу программных средств криптопровайдеров.

В мире ведутся научные исследования по разработке информационных систем и методов, алгоритмов и систем обеспечения безопасности информации в них. Эти исследования направлены на изучение существующих методов и алгоритмов криптографической защиты информации, создание криптографических модулей, отвечающих стандартам, и исследование угроз для криптографических модулей. Тем не менее, разработка и совершенствование алгоритмов, методов и средств обеспечения защиты информации от киберугроз, которые с каждым годом возрастают, считаются важными задачами.

В нашей республике реализуются комплексные меры, направленные на защиту информационных систем от киберугроз и обеспечение целостности, конфиденциальности и доступности информации. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017 — 2021 годах определены задачи, в частности "сбор, анализ и накопление данных о современных угрозах информационной безопасности, выработку рекомендаций и предложений по оперативному принятию эффективных организационных и программно-технических решений, обеспечивающих предотвращение актов незаконного проникновения в информационные системы, ресурсы и базы данных государственных органов и организаций". При реализации этих задач необходимо создание криптопровайдера, поддерживающего национальные криптографические алгоритмы и обеспечение эффективного управления криптографическими ключами.

Данное диссертационное исследование, в определенной степени, служит выполнению задач, предусмотренных указом Президента Республики Узбекистан № УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», постановлением Президента Республики Узбекистан № ПП-4024 от 21 ноября 2018 года «О мерах по совершенствованию системы контроля за внедрением

информационных технологий и коммуникаций, организации их защиты», а также в других нормативно-правовых документах, принятых в данной сфере.

Соответствие исследований приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в соответствии приоритетным направлениям развития науки и технологий в Республике Узбекистан IV. «Информатизация и развитие информационно–коммуникационных технологий».

Степень изученности проблемы. Научные исследования, направленные на разработку моделей, алгоритмов и средств криптографической защиты информации, проводятся рядом ученых по всему миру. Y. Ahmad[1] провел исследование CNG (Cryptography API: Next Generation) криптопровайдеров Windows и анализ алгоритмов, которые они поддерживают. Z. Lina[2] провела исследование архитектуры криптопровайдера хранения ключей CNG в операционной системе Windows, а также создания этих типов криптопровайдеров. K. Lee, H. Lee, Y. Lee, K. Yim, J. Park, I. You, I. Oh, S. Lee анализировали механизма хранения ключей библиотек CNG[3], безопасности библиотек CNG, угроз к библиотекам CNG[4], процессов обмена по протоколу SSL, а также свойств и структур интерфейса CNG. Для криптографической защиты информации разработаны CNG криптопровайдеры "Microsoft Primitive Provider", "Microsoft Software Key Storage Provider", "Microsoft SSL Protocol Provider", "Microsoft Smart Card Key Storage Provider" (Microsoft, США), а также криптопровайдеры "ViPNet CSP" (ИнфоТеКС, Россия), "КриптоПро CSP" (КриптоПро, Россия), "Signal-COM CSP" (Сигнал-КОМ, Россия), "Валидата CSP" (Валидата, Россия), "Лисси CSP" (ЛИССИ-Софт, Россия), "Tumar CSP" (Гамма Технологии, Казахстан), "AVEST CSP" (АВЕСТ, Беларусь), "IIT" (IIT, Украина).

По созданию интеллектуальных систем защиты информации, методов и средств защиты информации, генерации случайных чисел, разработке и анализа алгоритмов шифрования, хэш-функции и электронной цифровой подписи, а также разработке концептуальной модели контроля доступа в компьютерных системах, исследования проводились научными коллективами под руководством Т.Ф.Бекмуродова[5], М.М.Арипова, С.К.Ганиева[6],

---

[1] Y. Ahmad. "A study on algorithms supported by CNG of Windows Operating System". // International Journal of Modern Engineering Research (IJMER). 2012, Vol.2, Issue.1, pp. 276-280.

[2] Z. Lina. "Design and Implementation of KSP on the Next Generation Cryptography API". // International Conference on Medical Physics and Biomedical Engineering (ICMPBE), vol. 33, pp. 1640-1646, Sep. 2012.

[3] K. Lee, H. Lee, Y. Lee and K. Yim, "Analysis on the Key Storage Mechanism of the CNG Library" // 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, 2016, -pp. 499-502.

[4] K. Lee, I. Oh, S. Lee, K. Yim. Vulnerability Analysis on the CNG Crypto Library. // The Journal of Korean Institute of Communications and Information Sciences. Vol.42 No.04, -pp. 838-847.

[5] Bekmuratov T.F., Botirov F.B. Development of structures of intellectual information protection system, Chemical technology. control and management. 2019. vol. 6, No. 90, -pp. 63-71.

[6] Ganiyev S.K., Khudoykulov Z.T., Halimtaeva I.U., Computer's source based (Pseudo) random number generation. //2017 Information Science and Communications Technologies (ICISCT), Tashkent 2017, –pp. 1-6.

Г.Х.Хамдамова[1], Р.Д.Алоева[2], М.М.Каримова[3], П.Ф.Хасанова, А.В.Кабулова[4], Б.Ф.Абдурахимова[5], Г.У.Жураева[6], Д.Я.Иргашева[7].

Вместе с тем, недостаточно исследованы методы реализации криптографических алгоритмов в операционной системе, а также разработка криптопровайдеров, поддерживающих алгоритмы стандартов O'zDSt 1106:2009 – функция хеширования, O'zDSt 1105:2009 – алгоритм шифрования данных, O'zDSt 1092:2009 – процессы генерации и проверки электронной цифровой подписи.

Связь темы диссертации с научно-исследовательскими работами высшего учебного заведения, в которой выполнялась диссертация. Диссертация выполнена в рамках проекта Национального университета Узбекистана имени Мирзо Улугбека ОТ-2018-Atex-546 «Создание мобильных приложений для операционных систем Android и IOS» (2018-2020 гг.).

Целью исследования является обеспечение эффективного управления ключами и создание криптопровайдеров для криптографической защиты информации, поддерживающих алгоритмы стандартов "O'zDSt 1106:2009 – функция хеширования", "O'zDSt 1105:2009 – алгоритм шифрования данных", "O'zDSt 1092:2009 – процессы формирования и проверки электронной цифровой подписи".

Задачи исследования состоят в следующем:

создание алгоритма выработки общего секретного ключа с использованием пары ключей первого алгоритма стандарта O'zDSt 1092:2009;

разработка алгоритма управления доступом к ключам алгоритма O'zDSt 1092:2009;

разработка метода обеспечения безопасности ключей алгоритма O'zDSt 1092:2009;

анализ угроз безопасности криптопровайдеров, разработка модели угроз и оценка угроз;

создание криптопровайдера, поддерживающего алгоритмы стандартов O'zDSt 1105:2009, O'zDSt 1106:2009 и O'zDSt 1092:2009;

---

[1] Askar T. Rakhmanov, Rustam Kh. Khamdamov, Komil F. Kerimov, Shukhrat K. Kamalov, Automatic Vulnerability Detection Algorithm for the SQL-Injection. // Journal of Automation and Information Sciences. 2019. Vol. 51, Issue 7. -pp. 47-54.

[2] Aloev R.D., Nurullaev M. Software, algorithms and methods of data encryption based on national standards. // IIUM Engineering Journal. 2020, Vol. 21, issue 1, -pp. 142-166.

[3] Kodirov Z.Z., Karimov M.M., Tashev K.A., Gulomov Sh.R., Islomova M.X. Artificial Intelligence, Ensuring Information Security In Virtual Robots And Extensive Use Of Smart Systems. // American Journal of Engineering and Technology. 2020. Vol 2 No 08. -pp. 28-38.

[4] Кабулов А.В., Варисов А.А., Каландаров И. Оценка рисков информационной безопасности и обеспечение конфиденциальности информационных ресурсов. // Проблемы информатики и энергетики. 2017. — №6.— С.27–36.

[5] Abdurakhimov B.F., Sattarov A.B. An algorithm for constructing S-boxes for block symmetric encryption // International Journal: "Universal Journal of Mathematics and Applications". 2018. Vol.1, No.1 -pp. 29-32.

[6] Juraev G.U., Ikramov A.A., Marakhimov A.R. About differential cryptanalysis algorithm of block encryption "Kuznyechik". // International Journal of Advanced Research in Science, Engineering and Technology. 2019. Vol. 6, Issue 2. —pp. 8164-8169.

[7] Irgasheva D., Khurramov D., Rustamova S., Approaches to Formalizing the Access Control System. // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent 2021, –pp. 1-4.

создание криптографического модуля, позволяющего распознавать цифровые сертификаты, созданные на основе алгоритмов O'zDSt 1106:2009 и O'zDSt 1092:2009, операционной системой Windows.

Объектом исследования является криптопровайдеры, выполняющих криптографические операции в операционных системах Windows.

Предметом исследования является методы управления ключами и создание криптопровайдеров для обеспечения криптографической защиты информации, поддерживающих алгоритмы стандартов "O'zDSt 1106:2009 – функция хеширования", "O'zDSt 1105:2009 – алгоритм шифрования данных", "O'zDSt 1092:2009 – процессы формирования и проверки электронной цифровой подписи".

Методы исследования. В исследовании использованы методы криптографической защиты информации, теории чисел, моделирования, системного программирования и объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

создан алгоритм выработки общего секретного ключа с использованием пары ключей первого алгоритма стандарта O'zDSt 1092:2009 для симметричных криптосистем;

разработан метод, повышающий безопасность ключей пользователей с различными привилегиями на компьютере на основе хеш функции;

на основе технологии веб-сервиса разработан алгоритм эффективного управления доступом ключами электронной цифровой подписи на мобильном устройстве;

разработана модель угроз для криптопровайдеров на основе методологии STRIDE, а также классифицированы и оценены угрозы информационной безопасности на основе методологии DREAD;

разработан программное средство "Криптопровайдер хеша, подписи и симметричного шифрования", обеспечивающее защиту от киберугроз, направленных на нарушение конфиденциальности и целостности информации, с использованием алгоритмов национальных стандартов O'zDSt 1105:2009, O'zDSt 1106:2009 и O'zDSt 1092:2009 посредством стандартных интерфейсов криптографии операционной системы Windows;

путем интеграции со службой сертификации Active Directory операционной системы Windows создано программное средство "Криптопровайдер хранилища ключей", обеспечивающий эффективное управление ключами алгоритмов стандарта O'zDSt 1092:2009.

Практические результаты исследования заключаются:

создана возможность защиты документов в приложениях Microsoft Office с использованием национальных алгоритмов;

создан модуль, обеспечивающий распознавание цифровых сертификатов, созданных с использованием алгоритмов O'zDSt 1106:2009 и O'zDSt 1092:2009, операционной системой Windows;

создана возможность формирования «Инфраструктуры открытых ключей», поддерживающей алгоритмы O'zDSt 1106:2009 и O'zDSt 1092:2009, с использованием Службы сертификации Active Directory.

Достоверность результатов исследования. Достоверность научных результатов основана взаимодействии созданных криптопровайдеров с операционной системой, а также на результатах экспериментов над алгоритмами, разработанными при реализации программного комплекса.

Научная и практическая значимость результатов исследования.

Научная ценность результатов исследования подтверждается тем, что разработан алгоритм, позволяющий выработать общий секретный ключ, а также метод управления доступом ключей и безопасного хранения ключей.

Практическая значимость результатов исследования заключается в использование единого ключа в нескольких информационных системах для обеспечения криптографической защиты информации, поддержка операционной системой Windows цифровых сертификатов, созданных на основе алгоритмов O'zDSt 1092:2009 и O'zDSt 1106:2009, а также возможность использования криптопровайдеров через интерфейс CNG.

Внедрение результатов исследования.

На основании полученных научных результатов по обеспечению криптографической защиты информации в рамках диссертационных исследований:

Метод и программный комплекс для доступа к ключам электронной цифровой подписи использовались в проекте «Разработка методов и инструментов для улучшения услуг безопасности инфраструктуры открытых ключей Республики Узбекистан» в Центре научно-технических и маркетинговых исследований ГУП «UNICON.UZ» (справка Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 ноября 2021 года №33-8/8538). Использование результатов научного исследование, повышают эффективности использования криптографических методов при устранении угроз, направленных на нарушение конфиденциальности и целостности данных, а также данное программное обеспечение позволило зарегистрировать имеющиеся ключи в нашей республике.

Алгоритм выработки общего ключа, модель угроз и программное обеспечение были внедрены в Ташкентском университете информационных технологий имени Мухаммада Аль-Хорезми в рамках проекта «BV F4-023» «Исследование проблем управления инцидентами и кибератаками в распределенных информационных системах» (справка Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 ноября 2021 года №33-8/8538). Использование результатов научного исследования позволило на 10-12% повысить эффективность использования криптографических методов при устранении угроз нарушения конфиденциальности и целостности данных.

Программное обеспечение криптографической защиты информации и управления цифровыми сертификатами, созданное на основе алгоритмов

O‘zDSt 1092:2009 и O‘zDSt 1106:2009, внедрено в ООО «SMART SOFTWARE» в проекте «Информационная система автоматизации бизнес процесса “Кишлок курилиш инвест”» (справка Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 ноября 2021 года №33-8/8538). Результаты научного исследования были применены для обеспечения конфиденциальности и целостности информации и позволили вдвое снизить затраты на обеспечение криптографической защиты информации в информационной системе.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 11 научно-практических конференциях, в том числе на 5 международных и 6 республиканских.

Публикация результатов исследования. По теме диссертации опубликовано 20 научных работ, из них 7 входят в перечень научных изданий, предложенных Высшей аттестационной комиссией Республики Узбекистан для защиты диссертаций доктора философии, из них 2 опубликована в зарубежных журналах и 5 в республиканских научных изданиях.

А также получены 2 свидетельства о регистрации программных средств для ЭВМ.

Структура и объем диссертации: Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 120 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и востребованность темы диссертации, определено соответствие исследования приоритетным направлениям развития науки и технологий республики. Приведен обзор зарубежных научных исследований по теме диссертации и оценена степень изученности проблемы, сформулированы цели и задачи, выявлены объект и предмет исследования, изложены научная новизна и практические результаты исследования, раскрыта теоретическая и практическая значимость полученных результатов, даны сведения о внедрении результатов исследования, об опубликованных работах и о структуре диссертации.

Первая глава диссертации **«Криптографические стандарты, интерфейсы и проблемы реализации алгоритмов в операционных системах»** состоит из трех параграфов. В первом параграфе описано необходимость внедрения криптографических алгоритмов в операционную систему, исследовано криптопровайдеры, созданные ведущими мировыми компаниями, анализировано их скорость шифрования и хеширования данных, а также оценено их надежность. Во втором параграфе анализировано криптографические стандарты и проведено сравнительный анализ криптографических интерфейсов. В третьем параграфе описаны требования к создаваемым криптопровайдерам и проблемы реализации криптографических алгоритмов в операционных системах.

Вторая глава диссертации **«Создание эффективных методов и алгоритмов управления криптографическими ключами»** состоит из трех параграфов.

В первом параграфе второй главы разработан алгоритм выработки общего секретного ключа на основе пары ключей первого алгоритма O'zDSt 1092:2009. Введены следующие обозначения:

(U_{az}, X_{az}) – закрытий ключ пользователя A;

(Y_{ao}, Z_{ao}) – открытий ключ пользователя A;

(U_{bz}, X_{bz}) – закрытий ключ пользователя B;

(Y_{bo}, Z_{bo}) – открытий ключ пользователя B;

K_a – выработанный секретный ключ пользователем A;

K_b – выработанный секретный ключ пользователем B;

L – длина генерируемого симметричного ключа в битах.

Основные шаги алгоритма:

Шаг 1. Пользователь A вычисляет $K1$ и $K2$ по следующих формулах соответственно:

$$K1 \equiv Y_{bo}^{\backslash U_{az}} (mod\ p).$$
$$K2 \equiv Z_{bo}^{\backslash X_{az}} (mod\ p).$$

Шаг 2. $K = K1\ xor\ K2$.

Шаг 3. $K_a \equiv K (mod\ 2^L)$.

Шаг 4. Получатель B вычисляет $K1$ и $K2$ по следующих формулах соответственно:

$$K1 \equiv Z_{ao}^{\backslash X_{bz}} (mod\ p).$$
$$K2 \equiv Y_{ao}^{\backslash U_{bz}} (mod\ p).$$

Шаг 5. $K = K1\ xor\ K2$.

Шаг 6. $K_b \equiv K (mod\ 2^L)$.

Здесь, $K_a = K_b$.

Обозначаем с K_u выработанные ключи K_a и K_b. Здесь, K_u – общий секретный ключ. Выработанный секретный ключ K_u можно сразу использовать для шифрования существующего симметричного ключа K_s, или хешировать K_u по следующей формуле и использовать как K_s:

$$K_s = h(K_u)$$

где h – функция хеширования.

Во втором параграфе второй главы представлена модель угроз для криптопровайдеров на основе методологии STRIDE, а также оценка угроз на основе методологии DREAD. Угрозы обозначаются как $t_i \in T$, $i = \overline{1, N_t}$, защищаемые ресурсы обозначаются как $m_j \in M$, $j = \overline{1, N_m}$, а также меры защиты обозначаются как $h_k \in H$, $k = \overline{1, N_h}$. Каждую угрозу описываем через 5 атрибутов $(D_i; R_i; E_i; A_i; Di_i)$. Здесь, $D_i, R_i, E_i, A_i, Di_i \in \{1; 2; 3\}$ оценка каждой угрозы согласно методологии DREAD. На основе 5 атрибутов угрозы вычисляется уровень угрозы $X(t_i)$ по следующей формуле:

$$X(t_i) = (D_i + R_i + E_i + A_i + Di_i).$$

Рейтинг *i*-угроз, $TR(t_i) \in$ {высокий, средний, низкий}, вычисляется по следующей формуле:

$$TR(t_i) = \begin{cases} \text{высокий}, & \text{если } 12 \le X_i \le 15, \\ \text{средний}, & \text{если } 8 \le X_i \le 11, \\ \text{низкий}, & \text{если } 5 \le X_i \le 7. \end{cases}$$

Относительная важность *i*-угроз, $TN(t_i)$, вычисляется по следующей формуле:

$$TN(t_i) = \frac{X(t_i)}{\sum_{j=1}^{N_t} X(t_j)},$$

$$\sum_{i=1}^{N_t} TN(t_i) = 1.$$

Связь между угрозами, ресурсами и мерами защиты может быть выражена в виде графа:

$$G(V,E) = \langle V,E \rangle, V = T \cup M \cup H, T \neq \emptyset, M \neq \emptyset, H \neq \emptyset,$$
$$E \subseteq T \times M \cup T \times H \cup M \times H$$

Здесь, вершины графа будет 3 типов: угрозы, ресурсы и меры защиты. Ребро (t_i, m_j) ребро означает, что существует угроза t_i для ресурса m_j. (t_i, m_j, h_k) вектор означает, что для ресурса m_j существует мера защита h_k от угрозы t_i.

Определяем функцию $\omega(t_i, m_j)$ представляющую угрозы ресурсу:

$$\omega(t_i, m_j) = \begin{cases} 1, \text{если существует угроза } t_i \text{ для } m_j \\ 0, \quad \text{иначе.} \end{cases}$$

$f(t_i, m_j)$: $E' \times H \to [0,1]$ отражение, если для ресурса m_j существует хотя бы одно мера защиты h_k от угрозы t_i, тогда $f(t_i, m_j) = 0$, иначе $f(t_i, m_j) = 1$.

Значение риска $rb(m_j)$ для каждого ресурса m_j вычисляется по следующей формуле, не учитывающей угрозы с низким рейтингом:

$$rb(m_j) = \sum_{i=1}^{N_t} \begin{cases} 0, \text{если } TR(t_i) = \text{"низкий"}, \\ \omega(t_i, m_j) * TN(t_i), \text{иначе.} \end{cases}$$

Оценка риска *RB* для всех ресурсов или на уровне системы вычисляется по следующей формуле:

$$RB = \sum_{j=1}^{N_m} rb(m_j).$$

Для каждого ресурса m_j оценка риска после применения мер защиты $rbh(m_j)$ вычисляется по следующей формуле, не учитывающей угрозы со следующим рейтингом:

$$rbh(m_j) = \sum_{i=1}^{N_t} \begin{cases} 0, \text{если } TR(t_i) = \text{"низкий"}, \\ f(t_i, m_j) * rb(m_j), \quad \text{иначе.} \end{cases}$$

После применения защитных мер оценка риска *RBH* для всех ресурсов или на уровне системы вычисляется по следующей формуле:

$$RBH = \sum_{j=1}^{N_m} rbh(m_j).$$

Эффективность, достигаемая при применении меры защиты, вычисляется по следующей формуле:

$$SK = \frac{RB-RBH}{RB}.$$

В третьем параграфе второй главы разработан алгоритм управления доступом к криптографическому ключу. Предлагаемая архитектура системы доступа к ключам на мобильных устройствах состоит из 3-х модулей: криптографический модуль – C_c, принимающий запросы от прикладных приложений, криптографический модуль – C_m на мобильном устройстве и веб-сервис – W. Введем следующие обозначения:

E – функция шифрования асимметричного алгоритма;

E' – функция шифрования симметричного алгоритма;

D – функция расшифрования асимметричного алгоритма;

D' – функция расшифрования симметричного алгоритма;

$h(x)$ – функция хеширования;

M – данные для подписания;

H – хеш значения;

K_{ou} – открытый ключ пользователя;

K_{pu} – закрытый ключ пользователя;

K_{ow} – открытый ключ веб сервиса W;

K_{pw} – закрытый ключ веб сервиса W;

K_{ms} и K_{cs} – симметричные ключи;

L_f – логин пользователя в W, логином может быт номер телефона или адрес электронной почты;

App – прикладная программа;

W – промежуточный веб сервис для обеспечения взаимодействия между криптографическими модулями C_c и C_m. Здесь хранятся пользовательские сертификаты, имя пользователя и временный пароль пользователя. У каждого пользователя может быть несколько сертификатов.

Каждый пользователь сначала зарегистрируется в системе. Следующие процессы продемонстрирует взаимодействие модулей по шагам.

Процесс регистрации. Процесс регистрации осуществляется с помощью модуля C_m и веб сервиса W. Он включает в себя следующие шаги:

Шаг 1. На стороне C_m пользователь выбирает одну из операций {создать новую пару ключей, импортировать существующую пару ключей}.

Шаг 2. Пользователь вводит ПИН-код на стороне C_m.

Шаг 3. Если пользователь выбирает «Импортировать существующую пару ключей», переход к шагу 7, в противном случае переход к шагу 4.

Шаг 4. C_m генерирует новую пару ключей $\{K_{pu}, K_{ou}\}$. C_m шифрует закрытый ключ, и сохраняет $\{K'_{pu}, K_{ou}, H_k\}$ в хранилище.

Шаг 5. C_m генерирует запрос на подпись сертификата (CSR) и отправляет CSR в *Центр регистрации (RA)*.

Шаг 6. C_m устанавливает сертификат, полученный от RA, переход к шагу 9.

Шаг 7. C_m просит пользователя ввести пароль и импортирует пары ключей, зашифрованные в формате *PKCS#12*.

Шаг 8. C_m шифрует K_{pu}, сохраняет $\{K'_{pu}, K_{ou}, H_k$, сертификат$\}$ в хранилище.

Шаг 9. C_m просит пользователя ввести L_f, вычисляет $H = h(L_f)$, $S = E_{K_{pu}}(H)$ и отправляет {L_f, S, сертификат пользователя} на W.

Шаг 10. W проверяет, если $D_{K_{ou}}(S) = h(L_f)$ тогда переход к шагу 11, иначе возвращает "Неверные параметры".

Шаг 11. Если L_f не используется другим пользователем, тогда переход к шагу 16.

Шаг 12. W проверяет «Принадлежат ли эти существующие сертификаты, прикрепленные к L_f, этому пользователю или нет». Для этого W выбирает все сертификаты, прикрепленные к L_f, генерирует случайное число T, вычисляет $T' = E_{K_{ou}}(T)$, $S = E_{K_{pw}}(h(T'))$ и возвращает {T', S, список сертификатов} на C_m.

Шаг 13. C_m проверяет, если у него нету какой-либо сертификат, который находится в списке сертификатов, отправленный веб сервисом W, тогда переход к шагу 14, иначе он выбирает этот сертификат, если $h(T') = D_{K_{ow}}(S)$ тогда вычисляет $T = D_{K_{pu}}(T')$, $T' = E_{K_{ow}}(T)$, $S = E_{K''_{pu}}(h(T'))$ и отправляет {T', S, выбранный сертификат модулем C_m} на W, переход к шагу 15. Здесь, K''_{pu} - закрытый ключ выбранного сертификата модулем C_m.

Шаг 14. C_m показывает пользователю сообщение “Логин уже занять”. Переход к шагу 9.

Шаг 15. W проверяет, если $h(T') = D_{K_{ou}}(S)$ и $T = D_{K_{pw}}(T')$ тогда переход к шагу 16, в противном случае возвращает сообщение об ошибке «Недопустимые параметры».

Шаг 16. W регистрирует пользователя, сохраняет L_f и сертификат пользователя в базе данных, возвращает «Успешно» в качестве статуса регистрации, переход к шагу 17.

Шаг 17. Регистрация успешно завершена. C_m закрывает соединение с W.

Процесс формирования подписи. В процессе подписания участвуют все 3 модуля. Этот процесс включает в себя следующие шаги:

Шаг 1. *App* устанавливает соединение с C_c для подписания.

Шаг 2. C_c просит ввести L_f от пользователя.

Шаг 3. C_c генерирует одноразовый пароль P показывает его пользователю в виде QR-кода.

Шаг 4. C_m сканирует *QR код* и получает P. C_m проверяет, если у пользователя больше одного сертификата, C_m просит пользователя выбрать один из них, иначе использует тот.

Шаг 5. C_m просит пользователя ввести ПИН-код для доступа к закрытому ключу. C_m вычисляет $K = h(h(PINcode))$, если $H_k = h(K)$ тогда вычисляет $K_{pu} = D'_K(K'_{pu})$, иначе показывает сообщение “Неверный пинкод” и переход к шагу 5.

Шаг 6. C_m вычисляет $K_s = h(h(P))$, $H = h(K_s)$, $H' = E_{K_{ow}}(H)$, $K'_s = E_{K_{pu}}(h(H'))$.

Шаг 7. C_m отправляет {L, выбранный пользователем сертификат} на W.

Шаг 8. W генерирует случайное число T, вычисляет $T' = E_{K_{ou}}(T)$, $S = E_{K_{pw}}(h(T'))$, и отправляет $\{T', S\}$ на C_m.

Шаг 9. Если $h(T') = D_{K_{ow}}(S)$, тогда C_m вычисляет $T = D_{K_{pu}}(T')$, $T'' = E_{K_{ow}}(T)$, $S = E_{K_{pu}}(h(T''))$ и отправляет $\{L_f, T'', S, H', K'_s\}$ на W. Значения H' и K'_s были вычислены на шаге 6.

Шаг 10. W проверяет, если $h(T'') = D_{K_{ou}}(S)$ и $T = D_{K_{pw}}(T'')$ и $h(H') = D_{K_{ou}}(K'_s)$, тогда вычисляет $P' = D_{K_{pw}}(H')$, W устанавливает одноразовый пароль P' для L_f.

Шаг 11. C_c вычисляет $K_s = h(h(P))$, $H = h(K_s)$, $H' = E_{K_{ow}}(H)$, и отправляет $\{L_f, H'\}$ на W для аутентификации.

Шаг 12. W вычисляет $P' = D_{K_{pw}}(H')$ и проверяет, если L_f и P' правильно, тогда W возвращает сертификат пользователя на C_c, иначе возвращает "Логин и/или пароль неверен".

Шаг 13. Если C_c получает сообщение "Логин и/или пароль неверен" от W, тогда C_c показывает сообщение пользователю. Переход к шагу 2.

Шаг 14. C_c возвращает сертификат пользователя в *App*.

Шаг 15. *App* отправляет на C_c сертификат пользователя и M для хеширования.

Шаг 16. C_c вычисляет $H = h(M)$ и возвращает его в *App*, алгоритм хеширования определяется сертификатом для подписи.

Шаг 17. *App* отправляет H на C_c для подписи.

Шаг 18. C_c вычисляет $H'_c = E'_{K_s}(H)$ и отправляет $\{H'_c$, сертификат пользователя$\}$ на W. Значение K_s для C_c были вычислены на шаге 11.

Шаг 19. W отправляет $\{H'_c$, сертификат пользователя$\}$ на C_m.

Шаг 20. C_m получает $\{H'_c$, сертификат пользователя$\}$ от W.

Шаг 21. C_m запрашивает у пользователя разрешение на подписание.

Шаг 22. Если пользователь разрешает подписание, тогда C_m вычисляет $H = D'_{K_s}(H'_c)$, $S = E_{K_{pu}}(H)$, $S' = E'_{K_s}(S)$ и отправляет $\{S'$, "Успешно"$\}$ в качестве статуса подписание, иначе отправляет "Подписание отказано" в качестве статуса подписание на W. Значение K_s для C_m были вычислены на шаге 6.

Шаг 23. W передает результат, полученный от C_m, на C_c.

Шаг 24. C_c проверяет, если результат подписания "Успешно", тогда вычисляет $S = D'_{K_s}(S')$ и отправляет $\{S$, "Успешно"$\}$, иначе отправляет "Подписание отказано" на *App*.

Шаг 25. *App* проверяет, если статус "Успешно" тогда *App* использует S в качестве подписи.

Шаг 26. *App* закрывает соединение с C_c.

Шаг 27. C_c закрывает соединение с W.

Шаг 28. W удаляет P'.

Процесс проверки подписи. Процесс проверки подписи включает следующие шаги:

Шаг 1. *App* открывает соединение с C_c для проверки подписи.

Шаг 2. *App* отправляет на C_c сертификат пользователя и M для хештрования.
Шаг 3. C_c вычисляет $H = h(M)$ и возвращает H на *App*. Алгоритм хеширования определяется сертификатом пользователя.
Шаг 4. *App* отправляет $\{H, S,$ сертификат подписи$\}$ на C_c.
Шаг 5. C_c проверяет, если $H = D_{K_{ou}}(S)$ тогда C_c возвращает "Подпись верна", иначе возвращает "Подпись не верна" в качестве статуса проверки.
Шаг 6. *App* закрывает соединение с C_c.

Этот алгоритм позволяет использовать единую копию ключа, расположенную на мобильном устройстве, в информационных системах на других устройствах.

В третьей главе **«Создание криптопровайдеров, поддерживающих алгоритмы стандартов криптографической защиты информации»** приведены процессы разработки критопровайдера «ARH Primitive Provider», поддерживающего алгоритмы стандартов O'zDSt 1105:2009, O'zDSt 1106:2009 и O'zDSt 1092:2009, разработки критопровайдера хранилища ключей для управления ключами алгоритмов стандарта O'zDSt 1092:2009, разработка модуля поддержки цифровых сертификатов, созданные на основе алгоритмов O'zDSt 1106:2009 и O'zDSt 1092:2009.

Метод безопасного хранения ключей. Криптопровайдер «ARH Key Storage Provider» обеспечивает защиту ключей на основе "ПИН-кода" и без "ПИН-кода". Если указан ПИН-код, ключ шифруется по следующей формуле:

$$Ke = Eu(Kp, Kb)$$

где Kp – ключ шифрования, Kb – сгенерированный закрытый ключ, Eu – алгоритм шифрования O'zDSt 1105:2009.

Ключ шифрования Kp вычисляется по следующей формуле.

$$Kp = h_u(h_u(h_u(PINcode)))$$

где h_u – хеш функция O'zDSt 1106:2009.

Если ПИН-код не указан, шифрование закрытого ключа выполняется с помощью функции *CryptProtectData*.

Атрибуты «системный» и «скрытый» устанавливаются для каталога и файла, в котором хранится ключ. Доступ к каталогу, в котором расположены файлы ключей, предоставляется учетной записи системы и группе администраторов. Если ключ является ключом уровня пользователя, то вышеуказанные разрешения также предоставляются текущему пользователю.

Для работы с цифровыми сертификатами в системе разработано "*Расширение криптопровайдера*". После установки этого расширения, оно обрабатывает запросы операционной системы на цифровые сертификаты, созданные на основе алгоритмов O'zDSt 1106:2009 и O'zDSt 1092:2009, формирует запросы на выдачу нового сертификата, обеспечивает проверку подписи цифрового сертификата.

Четвертая глава **«Внедрение программного обеспечения крипто провайдеров "ARH Primitive provider" и "ARH Key storage provider"»** посвящена внедрении "ARH Primitive provider" и "ARH Key storage provider", которые поддерживают национальные криптографические алгоритмы защиты

информации. Приведены процессы создания «Инфраструктуры открытых ключей», поддерживающей алгоритмы "O'zDSt 1106:2009" и "O'zDSt 1092:2009", интеграция с криптопровайдером в приложениях Microsoft Office для обеспечения безопасности с использованием алгоритмов "O'zDSt 1105:2009" и "O'zDSt 1106:2009", оценка эффективности внедрения созданных криптопровайдеров, а также сравнительный анализ функций криптопровайдеров и других криптографических модулей (таблица 1).

Таблица 1. Сравнительный анализ функций криптопровайдеров и других криптографических модулей

№	Функция	ARH Primitive Provider, ARH Key Storage Provider (1-существует, 0-не существует)	Другие криптографические модули не являющимися криптопровайдерами (1-существует, 0-не существует)	Коэффициент использования (1-мало, 5-средний, 10-много)	A*K	B*K
		A	B	K		
1.	Создание, экспорт/ импорт, применение и удаление ключей алгоритмов стандарта O'zDSt 1092:2009.	1	1	10	10	10
2.	Аутентификация на основе ПИН-кода.	1	1	10	10	10
3.	Аутентификация без ПИН-кода.	1	0	1	1	0
4.	Поддержка пользовательских ключей.	1	1	10	10	10
5.	Формирование и проверка подписи по алгоритмам стандарта O'zDSt 1092:2009, симметричное шифрование по алгоритмам O'zDSt 1105:2009 и ГОСТ	1	1	10	10	10

	28147-89, хеширование данных по алгоритмам стандарта O'zDSt 1106:2009.					
6.	Обеспечить криптографические операции для служебных программ операционной системы.	1	0	1	1	0
7.	Обеспечение работы операционной системы цифровыми с сертификатами O'zDSt 1106:2009 и O'zDSt 1092:2009.	1	0	1	1	0
8.	Использование алгоритмов O'zDSt 1106:2009 и O'zDSt 1105:2009 для защиты документов в приложениях Microsoft Office.	1	0	1	1	0
9.	Совместное использование методов защиты операционной системы (управление привилегиями, изоляция ключевых процессов, шифрование с открытым ключом) и собственных методов криптопровайдера для обеспечения безопасности ключей.	1	0	1	1	0
10.	Выработки общего секретного ключа на основе ключей первого алгоритма стандарта O'zDSt 1092:2009 для алгоритмов симметричного шифрования.	1	0	1	1	0
11.	Создание инфраструктуры открытых ключей.	1	1	10	10	10
12.	Применение двухуровневой иерархической модели инфраструктуры открытых ключей.	1	1	10	10	10

13.	Применение многоуровневой иерархической модели инфраструктуры открытых ключей.	1	0	1	1	0
14.	Создание цифровых сертификатов для различных целей, создание цифровых сертификатов с нестатической структурой.	1	0	1	1	0
Итого					68	60

Su – общая эффективность обеспечении криптографической защиты информации при использовании созданных криптопровайдеров вычисляется следующим образом:

$$Su = \frac{\sum_{i=1}^{14} A_i * K_i - \sum_{i=1}^{14} B_i * K_i}{\sum_{i=1}^{14} A_i * K_i} * 100 = \frac{68 - 60}{68} * 100 \approx 12\%$$

ЗАКЛЮЧЕНИЕ

Диссертация посвящена анализу и разработку моделей, алгоритмов и программ криптографической защиты информации.

Основные результаты исследования заключаются в следующем:

1. Разработан алгоритм выработки общего ключа на основе пары ключей первого алгоритма O‘zDSt 1092:2009, который позволил шифровать существующие симметричные ключи в симметричных криптосистемах с использованием пары ключей первого алгоритма O‘zDSt 1092:2009.

2. Создан метод безопасного хранения ключей. Для хранения ключей служебных программ операционной системы и пользовательских ключей использовались разные методы. В результате только сами сервисы имеют доступ к своим ключам, а доступ к пользовательским ключам есть только у владельцев этих ключей.

3. Разработана модель угроз информационной безопасности криптопровайдеров разработан на основе методологии STRIDE. Выявлены потенциальные угрозы для модулей криптопровайдера, и угрозы были оценены на основе методологии DREAD. В зависимости от рейтинга угроз при разработке программного обеспечения учитывались эффективные меры защиты.

4. Создан алгоритм управления доступом к ключам, хранящимся на мобильном устройстве, с других устройств. В результате одна копия ключа, хранящаяся на мобильном устройстве, может использоваться в любом

количестве информационных систем без хранения копий на нескольких устройствах.

5. Разработан криптопровайдер, поддерживающий алгоритмы стандартов O‘zDSt 1106:2009, O‘zDSt 1105:2009 и O‘zDSt 1092:2009, и криптопровайдер хранилища ключей для управления жизненным циклом ключей электронной цифровой подписи.

6. Создан модуль поддержки цифровых сертификатов, созданных на базе алгоритмов O‘zDSt 1106:2009 и O‘zDSt 1092:2009, и модуль обеспечения безопасности документов в приложениях Microsoft Office с алгоритмами O‘zDSt 1105:2009 и O‘zDSt 1106:2009.

7. Разработанные криптопровайдеры вдвое снизить затраты на обеспечение криптографической защиты информации в информационных системах. За счет того, что криптопровайдеры интегрированы с операционной системой, а также предоставляемых функций, криптопровайдеры повышают эффективность использования криптографических методов на 10-12% при устранении угроз нарушения конфиденциальности и целостности данных.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES
DSc.13/30.12.2019.T.07.02 AT TASHKENT UNIVERSITY OF
INFORMATION TECHNOLOGIES
NATIONAL UNIVERSITY OF UZBEKISTAN

ALAEV RUHILLO HABIBOVICH

MODELS, ALGORITHMS AND PROGRAMS FOR CRYPTOGRAPHIC INFORMATION PROTECTION

05.01.05 – Methods and systems of information protection. Information security.

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON TECHNICAL SCIENCES

Tashkent-2022

The theme of dissertation of doctor of philosophy (PhD) on technical sciences was registered at the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan under number №B2019.2.PhD/FM388.

The dissertation has been prepared at National University of Uzbekistan named after Mirzo Ulugbek.

The abstract of the dissertation is posted in three languages (uzbek, russian, english (resume)) on the website (www.tuit.uz) and the "ZiyoNet" Information and educational portal (www.ziyonet.uz).

Scientific supervisor:	**Aripov Mersaid Mirsiddikovich** Doctor of Physical and Mathematical Sciences, Professor
Official opponents:	**Kerimov Komil Fikratovich** Doctor of Technical Sciences, Associate professor
	Sattarov Alijon Bozorboevich Doctor of Philosophy (PhD) in Physical and Mathematical Sciences
Leading organization:	**Scientific Engineering and Marketing Researches Center "UNICON.UZ"**

The defense of the dissertation will be held «27» August 2022 at 12^{00} at the meeting of Scientific council No. DSc.13/30.12.2019.T.07.02 at Tashkent University of Information Technologies (Address: 100084, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43, fax: (+99871) 23865-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resource Centre of Tashkent University of Information Technologies (is registered under No.2700). (Address: 100084, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

The abstract of dissertation was sent out on «17» August 2022 y.
(mailing protocol No. 6 on «17» August 2022 y.).

B.Sh. Makhkamov
Chairman of scientific council on award of scientific degrees, Doctor of Economical Sciences, Professor

E.Sh. Nazirova
Scientific secretary of scientific council on award of scientific degrees, Doctor of Technical Sciences, Docent

S.K. Ganiev
Chairman of scientific seminar under scientific council on award of scientific degrees, Doctor of Technical Sciences, Professor

INTRODUCTION (abstract of PhD thesis)

The aim of the research work is to provide efficient key management and create providers that support cryptographic protection of information using algoritms "O'zDSt 1106:2009 - hashing functions", "O'zDSt 1105:2009 - data encryption algorithm" and "O'zDSt 1092:2009 - signature and verification processes of digital signature".

The object of the research work is providers that perform cryptographic operations on Windows operating systems.

Scientific novelty of research work is as follows:

developed an algorithm for establishing a shared secret key based on a key pair of the first signature algorithm of the O'zDSt 1092:2009 standard for symmetric cryptosystem;

developed a method that increases the security of keys of users with different privileges on a computer based on a hash function;

based on the web service technology, an algorithm for effective control of access to electronic digital signature keys on a mobile device has been developed;

a threat model for crypto providers was developed based on the STRIDE methodology, and information security threats were classified and assessed based on the DREAD methodology;

a software tool of "Hash, signature and cipher provider" was developed, which provides protection against cyber threats aimed at violating the confidentiality and integrity of information, using the algorithms of the national standards O'zDSt 1105:2009, O'zDSt 1106:2009 and O'zDSt 1092:2009 through the standard cryptography interfaces of the Windows operating system;

by integrating with the Active Directory certification service of the Windows operating system, a software tool "Key storage provider" was created, which provides efficient keys management for algorithms of the O'zDSt 1092:2009 standard.

Implementation of the research results. Based on the scientific results obtained to ensure cryptographic protection of information within the framework of dissertation research:

The method and software for accessing electronic digital signature keys were used in the project "Development of methods and tools for improving security services for the public key infrastructure of the Republic of Uzbekistan" at the Center for Scientific, Technical and Marketing Research of the SUE "UNICON.UZ" (Certificate of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan dated November 30, 2021 No. 33-8/8538). Using the results of scientific research, increase the effectiveness of the use of cryptographic methods in eliminating threats aimed at violating the confidentiality and integrity of data, and this software made it possible to register existing keys in our republic.

The algorithm for generating a shared key, a threat model and software were implemented at the Tashkent University of Information Technologies named after Muhammad Al-Khorezmi within the framework of the BV F4-023 project "Research of incident and cyber attack management problems in distributed Information

Systems" (Certificate of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan dated November 30, 2021 No. 33-8/8538). The use of the results of scientific research has made it possible to increase the efficiency of using cryptographic methods by 10-12% in eliminating threats of violation of confidentiality and data integrity.

The software for cryptographic information protection and digital certificate management, created on the basis of the algorithms O'zDSt 1092:2009 and O'zDSt 1106:2009, was implemented at "SMART SOFTWARE" Ltd in the project «Information system for automating the business process "Qishloq Qurilish invest"» (Certificate of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan dated November 30, 2021 No. 33-8/8538). The use of the results of scientific research was applied to ensure the confidentiality and integrity of data, which made it possible to reduce the cost of ensuring cryptographic protection of information in information systems by two times.

The structure and volume of the thesis: The thesis consists of an introduction, four chapters, conclusion, a list of used literature and applications. The volume of the thesis is 120 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (1 часть; part 1)

1. Alaev R.H. Applying Custom Algorithms in Windows Active Directory Certificate Services. // International Journal of Advanced Computer Science and Applications. 2021. Vol. 12, No. 7. —pp. 568-577. DOI: 10.14569/IJACSA.2021.0120765. (№3, Scopus; IF=1.09).
2. Арипов М.М., Алаев Р.Х. Алгоритм выработки общего секретного ключа на основе пары ключей первого алгоритма электронной цифровой подписи O'zDSt 1092:2009. // Проблемы вычислительной и прикладной математики. — 2021. — № 3(33). — С. 116–123. (05.00.00; №23).
3. Aripov M.M., Alaev R.H. Design and implementation the signature provider of the algorithm O'zDSt 1092:2009. // International Journal of Advanced Research in Science, Engineering and Technology. 2019. Vol. 6, Issue 3. —pp. 8367-8375. (05.00.00; №8).
4. Aripov M.M., Alaev R.H. Distributed system model for key management. // ТАТУ хабарлари. — 2019. — № 1(49). — С. 86–91. (05.00.00; №31).
5. Алоев Р.Д., Алаев Р.Х., Нуруллаев М.М. Разработка криптографического провайдера на основе национальных стандартов. // ЎзМУ хабарлари. — 2013. — № 2. — С. 32–35. (01.00.00; №8).
6. Алаев Р.Ҳ. Маҳаллий криптопровайдер архитектураси ҳақида. // ЎзМУ хабарлари. — 2013. — № 2. — С. 28–32. (01.00.00; №8).
7. Алоев Р.Д., Алаев Р.Ҳ., Нуруллаев М.М. Средство криптографической защиты информации NUUz CSP. // ЎзМУ хабарлари. — 2016. — № 2(2). — С. 70–82. (01.00.00; №8).

II бўлим (2 часть; part 2)

8. Aripov M.M., Alaev R.H. Research of the application of the new cryptographic algorithms: applying the cipher algorithm O'zDSt1105:2009 for MS office document encryption. In Proceedings of the 5th International Conference on Engineering and MIS (ICEMIS '19). 2019. Association for Computing Machinery, USA, -pp. 1–7. DOI:10.1145/3330431.3330434 (**№3, Scopus**).
9. Aripov M.M., Alaev R.H. Design and implementation of the hash provider of the hash algorithm O'zDSt 1106:2009. // Proceedings of ADYPU "2nd International Conference on Enhancement and Innovations in Exploring Engineering (ICEIEE-2019)". Kuala Lumpur, Malaysia 2019, July 12. –pp. 109-112.
10. Alaev R.H. An Algorithm for Generating a Shared Secret Key Based on a Key Pair of the First Signature Algorithm of the O'zDSt 1092:2009 Standard. // AIP Conference Proceedings "1st International Conference on Problems and Perspectives of Modern Science". 2022. Vol. 2432. Issue 1. (№3, Scopus; IF=0.40).

11. Алоев Р. Д., Алаев Р.Х. Структура программы криптопровайдера. // "Амалий математика ва ахборот хавфсизлиги" мавзусида Ўзбекистон Республикаси Олий ва ўрта махсус таълим вазирлиги миқёсида илмий-техник анжуман. Тошкент 2014 й., 28-30 апрель. –Б. 302-306.
12. Алаев Р.Ҳ. Янги авлод криптопровайдер интерфейси. // "Амалий математика ва ахборот хавфсизлиги" мавзусида Ўзбекистон Республикаси Олий ва ўрта махсус таълим вазирлиги миқёсида илмий-техник анжуман. Тошкент 2014 й., 28-30 апрель. –Б. 290-296.
13. Alayev R.H. UzCSP kriptoprovayderida kalitlarni boshqarish. // "Амалий математика ва информацион технологияларнинг долзарб муаммолари – Ал-Хоразмий 2016" халқаро конференция материаллари тўрлами. Тошкент 2016 й., 09-10 ноябрь. –Б. 133-136.
14. Алаев Р.Ҳ. Ташкилотлараро электрон ҳужжат айланишда криптопровайдерларнинг роли. // "Информатика, ахборот технологиялари ва бошқарув тизими: бугун ва келажакда" республика илмий-амалий конференция материаллари тўрлами. Навоий 2018 й., 20 апрель. –Б. 148-151.
15. Алаев Р.Ҳ. Windows операцион тизимида криптографик калитларни бошқариш. // International scientific conference "Information Technologies, Networks and Telecommunications" ITN&T-2021. Urgench 2021, may 25-26. –pp. 272-275.
16. Aripov M.M., Alaev R.H. Generating a certificate signing request (CSR) using Key storage provider and CertEnroll API. // "Амалий математика ва информацион технологияларнинг долзарб муаммолари – Ал-Хоразмий – 2018" халқаро анжуман тезислари тўплами. Тошкент 2018 й., 13-15 сентябрь. –Б. 61-62.
17. Алаев Р.Ҳ. Windows операцион тизимида O'zDSt 1092:2009 алгоритми асосида яратилган рақамли сертификатлар калитларини бошқариш. // "Амалий математика ва информацион технологияларнинг долзарб муаммолари" халқаро анжуман тезислари тўплами. Тошкент 2019 й., 14-15 ноябрь. –Б. 222.
18. Alaev R.H. Applying the O'zDSt 1106:2009 hash algorithm and the O'zDSt 1092:2009 signature algorithm in Active Directory Certificate Services. // International Uzbekistan-Malaysia Conference on "Computational models and technologies (CMT2020)". Tashkent 2020, August 24-25. –pp. 94-102.
19. Alayev R.H. O'zDSt 1092:2009 va O'zDSt 1106:2009 kruptoalgoritmlari asosida ishlab chiqarilgan raqamli sertifikatlarni boshqarish dasturi. // O'zbekiston Respublikasi Intellektual mulk agentligidan guvohnoma № DGU 12219, 20.08.2021.
20. Алаев Р.Ҳ. O'zDSt 1105:2009 симметрик алгоритми ёрдамида Microsoft Office ҳужжатларидан рухсатсиз фойдаланишни ҳимоя қилиш учун дастур. // Ўзбекистон Республикаси Интеллектуал мулк агентлигидан гувоҳнома № DGU 05884, 20.11.2018.

Автореферат «Муҳаммад ал-Хоразмий авлодлари» илмий журнали таҳририятида таҳрирдан ўтказилди ва ўзбек, инглиз, рус тилларидаги матнларнинг мослиги текширилди.

Босмахона лицензияси:

9338

Бичими: 84x60 $^{1}/_{16}$. «Times New Roman» гарнитураси.
Рақамли босма усулда босилди.
Шартли босма табоғи: 3,5. Адади 100 дона. Буюртма № 53/22.

Гувоҳнома № 851684.
«Tipograff» МЧЖ босмахонасида чоп этилган.
Босмахона манзили: 100011, Тошкент ш., Беруний кўчаси, 83-уй.