FRI-ONLINE-1-CCT2-02

TECHNOLOGIES FOR ENHANCEMENT OF MANAGEMENT SUSTAINABILITY OF SMART GRIDS TO IMITATION ATTACKS [18]

Prof. Mihail Iliev, DcS
Department of Telecommunications,
"Angel Kanchev" University of Ruse, Bulgaria
Tel.: +359 887544257
E-mail: miliev@uni-ruse.bg

Prof. Borislav Bedzhev, DcS
Communication networks and systems Department, "Vasil Levski" National Military University, Faculty "Artillery, AD and CIS", Shumen, Bulgaria
Tel.: +359 888745681
E-mail: bedzhev@abv.bg

Eng. Dobri Stoyanov
Communication networks and systems Department, "Vasil Levski" National Military University, Faculty "Artillery, AD and CIS", Shumen, Bulgaria
Phone: +359 897567136
E-mail: dobri_stoyanov@mail.bg

Eng. Stanimir Parvanov
Air Defense Department, "Vasil Levski" National Military University, Faculty "Artillery, AD and CIS", Shumen, Bulgaria
Phone: +359 885123955
E-mail: ssparvanov@gmail.com

Abstract: *The providing of high sustainability of electro-energy feeding system's management to remote cyberattacks is a very significant engineer problem, which could be successfully solved by applying of different technologies. Accounting this situation, in the paper the techologies for cybersecurity enhancement of the energy infrastructure management are analyzed and systematized. The substantiated conclusions could be useful in the development of the new smart grids.*

Keywords: *Cyberattack, Cybersecurity, Smart grid*

ВЪВЕДЕНИЕ

В последното десетилетие в икономически водещите страни в света се развива технологията Smart Grid (интелектуална (умна) мрежа). Умните мрежи позволяват на потребителите да са активна страна в доставянето и търговията с електрическа енергия (Erol-Kantarci, M., 2021). Тяхното реализиране стана възможно в резултат на напредъка в развитието на следните области:

- технологиите за измерване, наблюдение и управление на процесите в *енергоенергетическите* (ЕЕ) мрежи - например Индустриален Интернет на нещата (Internet of Things - IoT), „умни електромери", „умни асансьори", „умни домове" и др.;

- новите генераторни инсталации и устройства за съхранение на електрическа енергия: малки и микро *водно-електрически централи* (ВЕЦ), малки и микро *помпено-акумуласторни ВЕЦ* (ПАВЕЦ), *фото-волтаични* и *вятърни електрически централи* (ФвЕЦ и ВяЕЦ),

[18] Докладът е представен на заседание на секция 3.2 на 29 октомври 2021 с оригинално заглавие на български език: ТЕХНОЛОГИИ ЗА ПОВИШАВАНЕ УСТОЙЧИВОСТТА НА УПРАВЛЕНИЕТО НА УМНИТЕ МРЕЖИ КЪМ ИМИТАЦИОННИ АТАКИ

акумулаторни електрически батерии с голям капацитет (включително акумулаторите на електрическите коли);

- усъвършенстваните бързодействащи комутиращи устройства в ЕЕ мрежите;

- свръхнадеждните високоскоростни комуникационни и високопроизводителни компютърни системи.

Умните мрежи могат да намалят в значителна степен вредните последствия от човешката дейност върху околната среда чрез рационално управление на електрическите генериращи инсталации, както и на консумацията и преноса на електрическа енергия. За успешното изпълнение на тази мисия обаче в умните мрежи трябва да се използват технически решения, осигуряващи непрекъснатост и устойчивост на процесите на управление в реално време. Предвид на този факт задачите на настоящия доклад са:

1) да се направи анализ на заплахите за нормалното функциониране умните мрежи;

2) да се систематизират технологиите за повишаване устойчивостта на управлението на умните мрежи срещу имитационни атаки.

Тези задачи се решават в следващите два раздела на доклада.

ИЗЛОЖЕНИЕ

Анализ на заплахите за нормалното функциониране на умните мрежи

Данните, изнесени в информационните източници със свободен достъп, могат да се обобщят както следва.

Първо, агентите на заплахите за нормалното функциониране на умните мрежи в мирно време са терористични и криминални групи. Във военно време към посочените агенти на заплахата следва да се добавят диверсионните подразделения на армията на противника.

Второ, мотивите на терористичните и криминалните групи не са напълно идентични. По-конкретно, първата цел при атаките на елементите на ЕЕ мрежите е съществено нарушаване на нормалната им работа, способно да създаде условия за възникване на масово недоволство в отделни райони или в цялата страна. При това обаче крайната цел на терористичните групи е чувствително уронване на престижа или дори смяна на управляващия политическия режим, докато крайната цел на криминалните групи е получаването на възможно най-голям откуп.

Трето, най-широко приложение имат имитационните атаки, насочени към вредоносна промяна на режима на работа на автономните елементи на енергийната инфраструктура като например (Stoyanov, D., Bochev, L., Radev, I., 2021):

- изключване на слънчевите колектори през деня и включването им през нощта;

- активиране на перките на ветрогенераторите при много силен вятър, при което е възможно физическото им разрушаване;

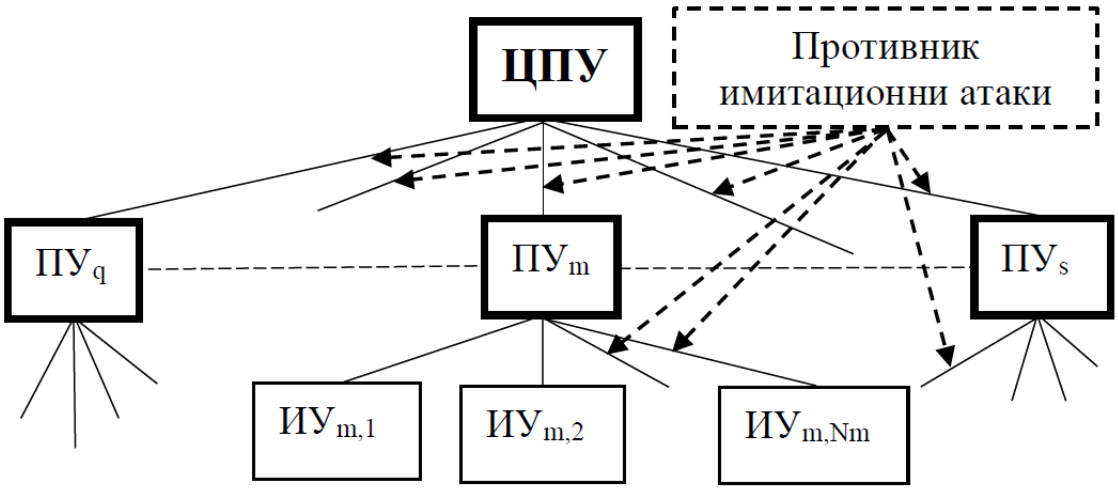
- установяване в ПАВЕЦ на режим „генериране“ през нощта и на режим „изпомпване“ през деня;

- предоставяне на по-малки количества електрическа енергия от необходимите или дори прекъсване електрозахранването на активни в момента потребители;

- продължително подаване на големи количества електрическа енергия през участъци на ЕЕ мрежата с недостатъчна пропускателна способност, при което възниква опасност от разтопяване на проводниците на ЕЕ линиите и дори разрушаване на трансформаторните подстанции;

- включване на електромерите в режим „дневна тарифа“ през нощта и т.н.

Четвърто, най-често структурите на подсистемите за управление на умните мрежи са йерархични с три нива (фиг. 1) (Erol-Kantarci, M., 2021).



Фиг. 1. Структура на подсистемата за управление на умна електроенергетическа мрежа

По-конкретно, на най-високото йерархично ниво е *централният пункт за управление* (ЦПУ), който контролира процесите в цялата умна мрежа. На второто йерархично ниво са *пунктовете за управление* (ПУ), наблюдаващи и коригиращи при необходимост режимите на работа на *изпълнителните устройства* (ИУ) в обособени участъци на умната мрежа. Към ИУ, заемащи най-ниското йерархично ниво, се отнасят: генериращите инсталации, ЕЕ линиите, трансформаторните подстанции, бързодействащи устройства на силовата електроника и електромашинни вентилни системи, както и датчици, осигуряващи получаването на своевременна (on-line) информация за режимите на работа на мрежата и състоянието на оборудването в конкретен географски район.

Тъй като в умните мрежи всички субекти на електроенергетическия пазар (генериращи инсталации, мрежи, потребители) вземат активно участие в процесите на предаване и разпределение на електроенергията, ЦПУ, ПУ и ИУ са свързани с една или повече комуникационни мрежи, осигуряващи преминаването на командна (от по-високите йерархични нива към по-ниските) и справочна, телеметрична (от по-ниските йерархични нива към по-високите) информация . В действителност информационният обмен „ЦПУ – ПУ“, „ПУ – ПУ“ и „ПУ – ИУ“ се осъществява с всички основни типове *комуникационни системи* (КС): *влакнесто-оптични* КС (ВОКС), мобилни КС, сателитни КС, класически телефонни системи и *КС, използващи ЕЕ линии* (КСИЕЛ, Power Line Communications - PLC). В случаите, когато ИУ са разположени в труднодостъпни местности или слабо урбанизирани територии, тогава не е възможно да се използват ВОКС и класически телефонни системи, а експлоатацията на мобилни КС е ненадеждна (Stoyanov, D., Bochev, L., Radev, I., 2021).

Тук следва специално да се отбележи, че информационните потоци в комуникационните мрежи, осигуряващи адаптивното функциониране на умните ЕЕ мрежи, са несиметрични. Действително, командните съобщения, изпращани от по-високите йерархични нива към по-ниските, съдържат по няколко байта информация, докато справочните и телеметрични данни, предавани от по-ниските йерархични нива към по-високите, могат да имат обем от стотици байтове.

Пето, в процеса на планиране на киберсигурността трябва да бъдат отчетени следните специфични особености на умните ЕЕ мрежи:

СО 1) работа в непрекъснат активен режим;

СО 2) задачата за съхраняване функционалността на системата има най-висок приоритет.

От изложените факти могат да се направят следните изводи:

И 1) Успешното решаване на проблема за осигуряване на непрекъснат активен режим на умните ЕЕ мрежи много съществено зависи от устойчивостта на тяхното управление към кибератаките на престъпни и терористични групи.

И 2) В мирно време типичните кибератаки срещу умните ЕЕ мрежи представляват имитационни атаки, целящи вредоносна промяна на режима на работа на автономните елементи на енергийната инфраструктура.

Технологии за повишаване устойчивостта на управлението на умните мрежи срещу имитационни атаки

Най-общият метод за повишаване устойчивостта на управлението на умните мрежи срещу имитационни атаки е шифрирането на всяко командно съобщение M преди то да бъде изпратено от ЦПУ към ПУ или от ПУ към ИУ (фиг. 1). Казано по-формално, от ЦПУ към ПУ или от ПУ към ИУ вместо командното съобщение M се изпраща шифротекстът $C(M)$:

$$C(M) = E_K(M). \quad (1)$$

В (1) символът $E_K(M)$ означава, че при шифрирането на командното съобщение M е използван криптографският ключ K.

Недостатък на този метод е уязвимостта към атаките „*неправилно повторение*“ и „*подмяна*“. Действително, в първия случай (атака „неправилно повторение“) агентът на заплахата (противникът) прехваща и записва в своя база данни различни шифрирани командни съобщения $C(M_1), C(M_2), \dots, C(M_k), \dots$, до ИУ в един участък на умната мрежа, след което ги изпраща към ИУ в други участъци. Такава атака се реализира лесно и има големи шансове за успех тъй като целесъобразните режими на работа на генериращите инсталации и на натоварване на ЕЕ линиите в различните сегменти на умната ЕЕ мрежа могат да бъдат коренно различни в един и същи времеви интервал.

Във втория случай (атака „подмяна“) агентът на заплахата (противникът) променя по случаен начин малко количество битове в шифрираните командни съобщения, записани в неговата база данни, след което изпраща модифицираните командни съобщения $C'(M_1), C'(M_2), \dots, C'(M_k), \dots$, към ИУ. Такава атака също се реализира лесно и има големи шансове за успех тъй като броят (количеството) на всички различни команди е от порядъка на няколко стотици, в резултат на което е твърде възможно поне едно от модифицираните командни съобщения да съвпадне с някое истинско шифрирано командно съобщение. Казано по-формално, вероятността да се сбъдне поне едно от събитията

$$C'(M_k) = C(M_l), l = const, k = 1, 2, \dots. \quad (2)$$

е неприемливо висока.

За избягване на атаките „неправилно повторение“ и „подмяна“ срещу умните ЕЕ мрежи е необходимо шифрираните командни съобщения да бъдат разширени така, че да бъде максимално трудно да се променят правдоподобно техният подател и тяхното съдържание. Най-общият метод за едновременното постигане на тези цели е въвеждането на *противоимитационно допълнение* (*ПИД*, *message authentication code - MAC*) към съобщението. В зависимост от дължината на ПИД са възможни следните две *основни технологии* (ОТ).

ОТ 1) Противоимитационното допълнение е самото командно съобщение, т.е. $MAC = M$, като при това обаче M и MAC се шифрират с различни криптографски ключове K_0 и K_1. Следователно, в тази ситуация, съобщението, изпратено от ЦПУ към ПУ или от ПУ към ИУ (фиг. 1) по комуникационния канал, има вида:

$$\{C(M), C(MAC)\}, \quad (3)$$

като тук $C(M) = E_{K_0}(M),\ C(MAC) = E_{K_1}(M)$.

След приемане на съобщението (3) ИУ изпълнява съдържащата се в него команда само ако дешифрираните стойности $D_{K_0}[C(M)]$ и $D_{K_1}[C(MAC)]$ съвпадат.

От изложеното се вижда, че основният недостатък на разгледаната основна технология ОТ 1 е двукратното увеличение на дължината L_M на командните съобщения. Тази отрицателна черта обаче не е съществена от практическа гледна точка поради следните причини.

Първо, дължината L_M на командните съобщения M не е голяма, тъй като те съдържат следните данни: номер на ПУ, номер на ИУ, време на изпращане и съдържание на командата. В резултат на това, интензивността на информационния поток от по-високите йерархични

нива към по-ниските нива на подсистемата за управление на умна ЕЕ мрежа е относително малък.

Второ, тъй като задачата за съхраняване функционалността на умната ЕЕ мрежа има най-висок приоритет, разширяването на командните съобщения с ПИД е напълно оправдана цена за постигането на много по-висока устойчивост към имитационни атаки. Действително, нека вероятността за успешно имитиране на едно командно съобщение M е $P_{succ}(M)$. Тогава вероятността за успешно имитиране на едновременно на командното съобщение M и $MAC = M$ е $P_{succ}^2 < P_{succ} < 1$.

Очевидно, в общия случай на прилагане на ОТ 1 могат да се използват $N_{MAC} \geq 1$ на брой ПИД. В резултат командното съобщение, изпратено от ЦПУ към ПУ или от ПУ към ИУ (фиг. 1), има вида:

$$\{C(M), C(MAC_1), C(MAC_2), \dots, C(MAC_{N_{MAC}})\}, \quad (4)$$

като тук $C(M) = E_{K_0}(M),\ C(MAC_1) = E_{K_1}(M), C(MAC_2) = E_{K_2}(M), \dots, C(MAC_{N_{MAC}}) = E_{K_{N_{MAC}}}(M)$.

Тъй като след приемане на командното съобщение (4) ИУ изпълнява съдържащата се в него команда само ако всички дешифрирани стойности $D_{K_0}[C(M)], D_{K_1}[C(MAC_1)], D_{K_2}[C(MAC_2)], \dots, D_{K_{N_{MAC}}}[C(MAC_{N_{MAC}})]$ съвпадат, вероятността за успешно имитиране едновременно на командното съобщение M и на всичките ПИД $MAC_1 = MAC_2 = \dots = MAC_{N_{MAC}} = M$ е $P_{succ}^{N_{MAC}+1} \ll 1$.

ОТ 2) Противоимитационното допълнение се получава чрез някакво преобразование T на командното съобщение M, т.е. $MAC = T(M)$. Най-често преобразованието T свива (компресира) командното съобщение до ПИД с малка дължина, което освен MAC е прието да се нарича още *маг* (*tag*).

В зависимост от характеристиките на преобразованието T, подходите, отнасящи се към групата на общите технологии ОТ 2, могат да се класифицират както следва.

ОТ 2.1) Противоимитационното допълнение представлява вектор-ред

$$MAC = \{b_1, b_2, \dots, b_{N_{tag}}\}, \quad (5)$$

чиито елементи изразяват някакви алгебрични съотношения (връзки) между символите на командното съобщение. По-конкретно, в сила са следните N_{tag} равенства:

$$b_i = F_i(m_{i1}, m_{i2}, \dots, m_{iN_i}), i = 1, 2, \dots, N_{tag}. \quad (6)$$

В (6) $G_{m,i} = \{m_{i1}, m_{i2}, \dots, m_{iN_i}\}, i = 1, 2, \dots, N_{tag}$ са подмножества на множеството на всичките символи $G_{m,M} = \{m_1, m_2, \dots, m_{N_M}\}$ на командното съобщение M, а $F_i, i = 1, 2, \dots, N_{tag}$ са алгебрични функции.

На практика тагът (5) е множеството на контролните и проверовъчните символи (битове), получено чрез използване на някакъв вид *шумоустойчиво кодиране* (*forward error correction - FEC*). В най-простия случай $N_{tag} = 1$ и b_1 е сумата по модул 2 на всички битове на командното съобщение M, т.е.

$$b_1 = m_1 + m_2 + \dots + m_{N_i}\ mod\ 2, \quad (7)$$

и, както се вижда, ПИД е просто код за проверка по четност.

От гледна точка на киберсигурността значително по-добри са следните варианти за практическо прилагане на ОТ 2.1.

Първо, тагът е *кодът за проверка на цикличния остатък* (*Cyclic Redundancy Check – CRC*). Действително, ако се използват по секретен график различни генераторни полиноми, чиито списък се пази в тайна и, освен това, времевият интервал за изпълнение на командата е ограничен, тогава агентът на заплахата (противникът) има малки шансове да формира правилно CRC кодът на фалшифицираното от него командно съобщение.

Второ, алгебричните функции $F_i(m_{i1}, m_{i2}, \dots, m_{iN_i}), i = 1, 2, \dots, N_{tag}$ в (6) са суми по модул 2, т.е.

$$b_i = m_{i1} + m_{i2} + \dots + m_{iN_i}\ mod\ 2, i = 1, 2, \dots, N_{tag}. \quad (8)$$

При това обаче всички подмножества $G_{m,i}, i = 1, 2, \dots, N_{tag}$ от символи на командното съобщение M имат общо сечение, т.е.

$$\bigcup_{i=1}^{N_{tag}} G_{m,i} \neq \emptyset. \quad (9)$$

Условието (9) гарантира, че промяната дори на един символ на командното съобщение M води до промяна на поне един символ на тага (5). Това съществено намалява шансовете на агента на заплахата (противникът) да формира правилно тагът на фалшифицираното от него командно съобщение, ако времевият интервал за изпълнение на командата е ограничен, а правилата за формиране на подмножествата $G_{m,i}, i = 1, 2, \dots, N_{tag}$ се пазят в тайна и се променят по секретен график.

ОТ 2.2) Противоимитационното допълнение е вектор-ред (5), който се получава в резултат на някакво криптографски устойчиво компресиране на командното съобщение M:

$$MAC = H(M), H \coloneqq \{0,1\}^{L_M} \to \{0,1\}^{L_{tag}}. \quad (10)$$

Към момента са разработени и практически внедрени редица алгоритми за криптографски устойчиво компресиране на съобщенията, които е прието да се наричат *хеш-функции*, а изходните им продукти – *хеш-значения* или *хеш-стойности*.

От най-общи позиции, изчисляването на хеш-стойността на съобщението M преминава през следните стъпки (ISO/IEC 9797, 2016):

Ст 1) Съобщението M се разбива на N_{bl} на брой блокове $B_1, B_2, \dots, B_{N_{bl}}$, с еднаква дължина L_{bl}, чиито типични стойности са $L_{bl} = 32, 64, 128, 256\ [b]$. При необходимост последният блок $B_{N_{bl}}$ се допълва с нули, така че неговата дължина да стане също L_{bl}.

Ст 2) Първият блок B_1 се шифрира със същия криптографски ключ K, както и съобщението M, при което се получава първата междинна хеш-стойност $H(1)$. Тя се сумира побитово по модул 2 с вторият блок B_2, полученият резултат отново се шифрира с ключа K, при което се получава втората междинна хеш-стойност $H(2)$ и т.н. По-формално тази процедура може да се представи във вида

$$\begin{aligned} H(1) &= E_K(B_1), \\ H(i) &= E_K[H(i-1) \boxplus_2 B_i\ ], i = 2, 3, \dots, N_{bl}, \\ H(M) &= H(N_{bl}). \end{aligned} \quad (11)$$

В (11) символът „$\boxplus_2$“ означава „побитово сумиране по модул 2“.

Следва специално да се отбележи, че тагът може да е някакво подмножество на символите на хеш-стойността $H(M)$, т.е. дължината на тага L_{tag} може да е по-малка от L_{bl}.

Очевидно, в общия случай на прилагане на ОТ 2 могат да се използват $N_{MAC} \geq 1$ на брой ПИД. В резултат командното съобщение, изпратено от ЦПУ към ПУ или от ПУ към ИУ (фиг. 1), има вида (4). Тъй като след приемане на командното съобщение (4) ИУ изпълнява съдържащата се в него команда само ако всички дешифрирани стойности $D_{K_0}[C(M)], D_{K_1}[C(MAC_1)], D_{K_2}[C(MAC_2)], \dots, D_{K_{N_{MAC}}}\left[C\left(MAC_{N_{MAC}}\right)\right]$ съвпадат, вероятността за успешно имитиране на едновременно на командното съобщение M и всичките ПИД $MAC_1, MAC_2, \dots, MAC_{N_{MAC}}$ също е от порядъка на $P_{succ}^{N_{MAC}+1}$.

При прилагането на ОТ 2 следва да бъдат взети под внимание следните особености.

Първо, тъй като таговете винаги се шифрират в ПУ преди да бъдат изпратени към ИУ, от теоретична гледна точка $C(MAC_1), C(MAC_2), \dots, C\left(MAC_{N_{MAC}}\right)$ са *електронни цифрови подписи* (*ЕЦП*) на командното съобщение M.

Второ, при ОТ 2.1 промяната дори на един символ на командното съобщение M винаги довежда до промяна на поне един символ на тага (5). Същевременно, правилата за формиране символите на тага са много ясни и това е уязвимост, от която може да се възползва всеки информиран (квалифициран) противник. В противоположност, при ОТ 2.2 промяната на един символ на командното съобщение M не винаги довежда до промяна на тага (5), тъй като обемът на пространството на всички възможни съобщения V_M е много по-голям от обема на пространството на всички възможни тагове

$$V_M = 2^{L_M} \gg 2^{L_{tag}} = V_{tag}. \quad (12)$$

От друга страна, правилата за формиране символите на тага са много сложни, което съществено затруднява дори високо квалифицираните противници.

Тъй като предимствата на ОТ 2.1 и ОТ 2.2 взаимно се допълват, целесъобразно е членовете на N_{tag}-елементното множество на таговете да бъдат формирани чрез използване и на двете основни технологии ОТ 2.1 и ОТ 2.2.

ЗАКЛЮЧЕНИЕ

В доклада са анализирани заплахите за нормалното функциониране умните електроенергетически мрежи и са систематизирани основните технологии за повишаване устойчивостта на тяхното управление срещу имитационни атаки. Обоснованите изводи могат да бъдат полезни при внедряването и развитието на умни електроенергетически системи в Република България.

БЛАГОДАРНОСТ

Този доклад е реализиран с подкрепата на Националната научна програма „Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТ в НОС)“, финансирана от Министерството на образованието и науката на България.

REFERENCES

Erol-Kantarci, M., (2021), “Smart Grid? Yes, AI Says: Bring It on!,” *IEEE CTN*, Issue: April 2021.

Stoyanov, D., Bochev, L., Radev, I., (2021). Approaches for cybersecurity enhancement of the energy infrastructure management. *Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty “Artillery, AD and CIS”, Shumen, Bulgaria* (***Оригинално заглавие:*** *Стоянов, Д., Бочев, Л., Радев, Ив., 2021. Подходи за повишаване киберсигурността при управлението на енергийната инфраструктура. Шумен: Сборник научни трудове на Международната научна конференция „Отбранителни технологии“ DefTech 2021, Факултет “Артилерия, ПВО и КИС”)*.

ISO/IEC 9797 (2016). Information technology - Security techniques - Message Authentication Codes (MACs), Part 1: Mechanisms using a block cipher, https://www.iso.org/standard/50375.html, Part 2: Mechanisms using a dedicated hash-function, https://www.iso.org/standard/75296.html.