ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ПРЕЗИДЕНТИ ҲУЗУРИДАГИ
ДАВЛАТ ХИЗМАТИНИ
РИВОЖЛАНТИРИШ АГЕНТЛИГИ

CYBER SECURITY CENTER

РАҚАМЛИ ГИГИЕНА

кибермаконда маълумотлар хавфсизлиги

МУНДАРИЖА

ЎЗБ

IT соҳаси ривожлангани сари киберхавфсизликни таъминлашнинг долзарблиги ошмоқда

Шавкат МИРЗИЁЕВ

ЎЗБ

Рақамли гигиена – бу нафақат тавсиялар мажмуи, балки замонавий ҳаётнинг ажралмас қисми бўлиб, у доимий эътибор ва ҳаракатни талаб қилади. Рақамли гигиена қоидаларига риоя этиш – кибермаконда шахсга доир маълумотларни ҳимоя қилишга, киберҳужумларни олдини олишга ва хавфсиз онлайн муҳит яратишга ёрдам беради, шунингдек барча фойдаланувчилар

ва ташкилотлар рақамли гигиенани аҳамиятини тушуниши ва ушбу соҳадаги билим ва кўникмаларини мунтазам равишда янгилаб туришлари талаб этилади

01
ҚИСМ

КИРИШ

1. Рақамли гигиена тушунчаси

2. Рақамли гигиенани аҳамияти

3. Давлат хизматчилари учун асосий тавсиялар

ЎЗБ

1 Рақамли гигиена тушунчаси

Рақамли гигиена

Рақамли гигиена киберхавфсизликка доир керакли кўникмаларни шакллантириш ҳамда кибертаҳдид ва хавфсизлик муаммоларини олдини олишга ёрдам беради. Рақамли гигиена баъзан шахсий гигиенага ҳам қиёсланади

Рақамли гигиенанинг асосий омиллари

Паролни хавфсиз бошқариш:

Аккаунтларда мураккаб ва такрорланмас пароллардан фойдаланиш ҳамда уларни доимий равишда алмаштириш лозим

Дастурий таъминотни янгилаш:

Операцион тизимлар ва иловаларни доимий янгилаб бориш билан хакерлар томонидан фойдаланилиши мумкин бўлган заифликларни бартараф этишга ёрдам беради

1 Рақамли гигиена тушунчаси

Икки даражали аутентификация (2FA)

Икки даражали аутентификациядан фойдаланиш хавфсизлик даражасини оширади, у фақат паролни эмас, балки шахсни тасдиқлашнинг иккинчи усулини ҳам талаб этади

Антивирус ва Firewall дастурларидан фойдаланиш:

Антивирус дастурлари вирус, троян ва бошқа дастурлар каби таҳдидларни аниқлаш, олдини олиш ва бартараф этишга хизмат қилса, Firewall эса ташқи таҳдидларни тармоқ ва компьютерларга киришини чеклайди

Wi-Fi хавфсизлиги:

Wi-Fi тармоғини мураккаб пароллар ва шифрлаш билан ҳимояланиши, ушбу тармоққа рухсатсиз киришни олдини олишга ёрдам беради

Шахсга доир маълумотларни ҳимоя қилиш:

Давлат хизматчилари ижтимоий тармоқларда ва очиқ манбаларда маълумотларни жойлаштиришга онгли равишда ёндашишлари керак. Шахсга доир маълумотларга киришни чеклаш учун махфийлик параметрларини созлаш муҳим аҳамиятга эга

Таҳдидларни аниқлаш:

Давлат хизматчиларининг кибертаҳдидлар тўғрисидаги билим ва кўникмаларини доимий ошириш киберҳужумлардан самаралироқ ҳимояланиш имкониятини беради

Шубҳали ҳавола ва иловалар:

Фишинг ҳужумлар ҳамда зарарли дастурлардан ҳимояланиш учун шубҳали ҳаволаларга кириш ва электрон почта орқали келиб тушган шубҳали иловаларни юклаб олишдан чекланиш

Рақамли гигиенанинг асосий омиллари:

Рақамли гигиена фақат шахсга доир маълумотларни ҳимоя қилишга эмас, балки рақамли технологиялардан кундалик ҳаётда хавфсиз ва масъулият билан фойдаланишга ёрдам беради

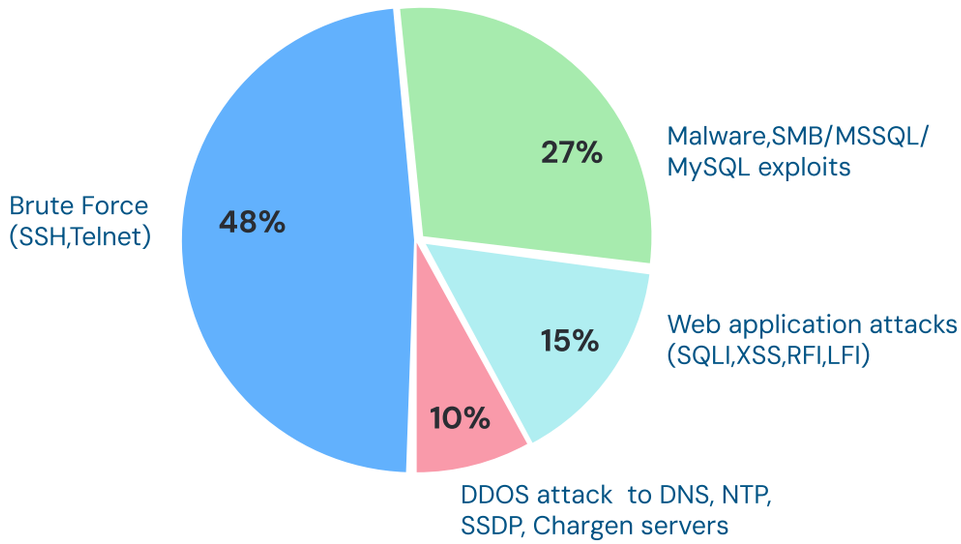
2 Рақамли гигиена аҳамияти

Давлат хизматчилари учун рақамли гигиена қоидаларига риоя этишлари ўта муҳим, сабаби давлат хизматчиларининг конфиденциал маълумотлардан нафақат иш фаолиятида, балки стратегик қарорларни қабул қилишда фойдаланишади. Рақамли гигиена тамойилларига риоя қилмасли шахсга доир маълумотларни чиқиб кетиши ва жиддий кибер таҳтидларга олиб келиши мумкин

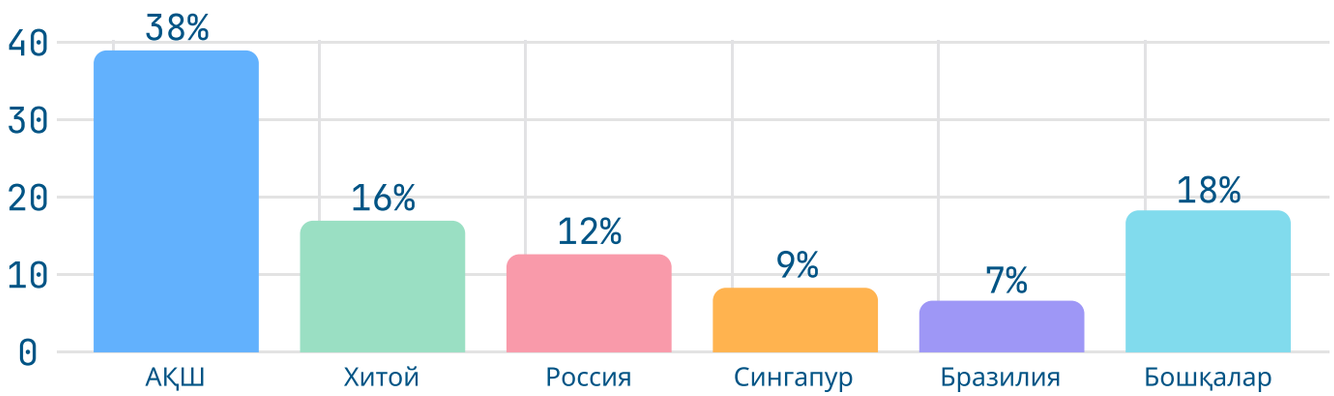
“.uz” доменида қайд этилган киберҳужумлар

2024 йил давомида "Honeypot*" тизимларига 70 миллиондан ортиқ киберҳужумлар амалга оширилди

Кўп тарқалган киберҳужум турлари:



Киберҳужумлар мамлакатлар кесимида:



*Honeypot – бу бузғунчиларнинг стратегиясини ўрганиш ва ҳақиқий хавфсизлик объектларига ҳужумларни амалга ошириш мумкин бўлган воситалар рўйхатини аниқлаш ресурси

2 Рақамли гигиена аҳамияти

Давлат хизматчилари учун рақамли гигиенани муҳимлиги

Конфиденциал маълумотларни ҳимоя қилиш:

Давлат хизматчилари шахсга доир маълумотлар, давлат ва молиявий сирлар ҳамда бошқа конфиденциал маълумотлардан фойдаланишда ахборот хавфсизлиги қоидаларига риоя этиш кўникмалари оширилади

Хавфсизлик ҳодисаларига бардошлилик:

Рақамли гигиена талабларидан амалиётда тўғри фойдаланиш хавфсизлик ҳодисаларини олдини олиш, уларнинг оқибатларини тезкор бартараф этишга имконият беради

Давлат ташкилотлари обрўсини сақлаб қолиш:

Рақамли гигиена қоидалари бузилиши фуқароларнинг давлат ташкилотларига бўлган ишончини сусайишига олиб келиши мумкин. Ушбу қоидаларга риоя қилиш давлат хизматчиларининг ўз вазифаларига масъулият билан ёндашишларини намоён этади

Рақамли саводхонликни ошириш:

Киберхавфсизлик ва рақамли гигиена бўйича доимий тренинглар давлат ходимларига янги таҳдидлар ва технологиялар тўғрисида хабардор бўлиш имконини беради

Киберҳужумларга қарши ҳимоя:

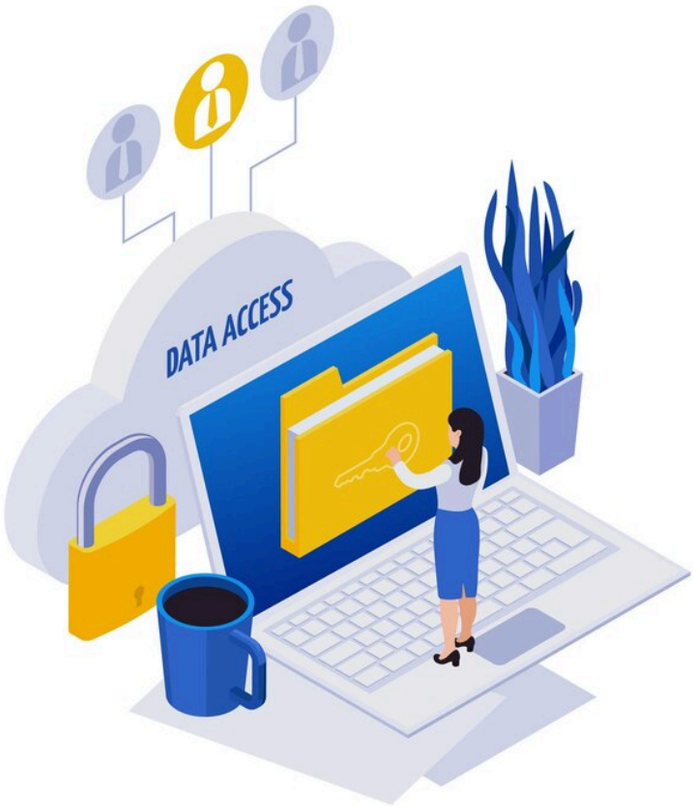
Фишинг, зарарли дастур ва хакерлик каби замонавий таҳдидлар киберхавфсизлик тўғрисида билим ва кўникмаларни оширишни талаб қилади. Мураккаб пароллар, икки факторли аутентификация ва дастурларни домий янгилаб бориш кибертаҳдидларни камайтиради

3 Давлат хизматчилари учун асосий тавсиялар

Давлат хизматчилари ўз функционал мажбуриятларини бажариш жараёнида ташкилотнинг “Ахборот хавфсизлиги сиёсати”да белгиланган тартиб-қоидаларига қатъий риоя қилишлари

Ахборот тизимлари ва ресурсларини юритишда ўз логин, пароль (шу жумладан ягона идентификация тизими - ONE ID маълумотлари), электрон рақамли имзо (ЭРИ), банк карта рақамлари, SMS орқали келган тасдиқловчи кодлар ва бошқалар тўғрисидаги маълумотларни учинчи шахсларга, шу қаторда бошқа ташкилот ва корхона вакилларига ошкора қилмаслик

Агар фирибгар қўнғироқ қилса, алдовга учманг!



Ташкилотда ахборот хвфсизлигини таъминлаш мақсадида қуйидаги ҳолатларда бевосита тегишли масъул бўлинмага дарҳол хабар бериш:

- маълумотларни асоссиз ошкор этилиши ва бунга йўл қўйган ходим(лар) тўғрисида;
- маълумотларга қизиқиш билдирган ва уларга эга бўлишга уринган ташкилотлар ёки учинчи шахслар тўғрисида;
- конфиденциал маълумотлар мавжуд бўлган қоғоз ёки электрон шаклининг йўқолиши тўғрисида;
- конфиденциал маълумотларни интернет сайтлари, форумлар, ижтимоий тармоқларда эълон қилиш бўйича;
- конфиденциал ҳужжатларни очиқ жойларда (принтерда, музокара хонасида) қолдириш ва бошқа ҳолатлар тўғрисида.

02
ҚИСМ

Рақамли гигиенанинг асосий омиллари

1. Киберҳужумлар

2. Фишингнинг асосий турлари

3. Зарарли дастурий таъминотлар

4. Маълумотларни чиқиб кетиши

ЎЗБ

1 Киберҳужумлар

Кибермаконда аппарат, аппарат-дастурий ва дастурий воситалардан фойдаланган ҳолда қасддан амалга ошириладиган, киберхавфсизликка таҳдид соладиган ҳаракат. Масалан: фишинг, паролларни бузиш, зарарли дастурий таъминотлар (вируслар, троянлар каби дастурлар) ва бошқалар ёрдамида (DDoS) амалга оширилади

Киберҳужумларнинг асосий турлари:

Фишинг

Бу алдаш йўли орқали конфиденциал маълумотларни олиш (ўғирлаш) усулидир. Фойдаланувчиларга сохта хабарлар юборилади (масалан, банк ёки бошқа ташкилотдан расмий хабарларга ўхшаш хатлар), уларни шахсий маълумотларини ошкор қилишга ёки зарарли ҳаволага ўтишга мажбурлаш мақсадида;

Огоҳ бўлинг! Фирибгарликнинг янги тури тарқалмоқда

1 Киберҳужумлар

Ҳужумлар (Man in the Middle)

Бундай ҳужумлар давомида хакерлар кўпинча фойдаланувчига сездирмаган ҳолда улар ва сервер ўртасидаги алоқани ушлаб қолади ҳамда ўзгартириб юборади. Бу ҳолат ҳимояланмаган Wi-Fi тармоқлари ёки бошқа заифликлар орқали содир бўлиши мумкин;

SQL-инъекциялар

Маълумотлар базаларига ҳужумлар – веб-иловалар кодидаги заифликлардан фойдаланиб, зарарли кодларни жорий қилиш орқали маълумотлар базасидаги маълумотларни ошкор қилиш ёки ўзгартиришга қаратилган ҳужум тури;

DDoS-ҳужумлар

Бундай ҳужумлар катта ҳажмдаги трафик орқали сервер ёки тармоқ инфратузилмаларининг юкламасини ошишига, натижада уларда жойлашган сайтлар ёки хизматларнинг носозликларга олиб келади;

Брутфорс

Бу усул барча мавжуд комбинацияларни танлаш орқали парол ёки шифрлаш калитини топишни назарда тутади. Бундай ёндашув фишинг ёки ижтимоий муҳандислик каби усуллар қўл келмаган ҳолларда ҳимояланган аккаунтлар, тизимлар ёки шифрланган маълумотларни бузиш учун қўлланилади;

Ижтимоий муҳандислик

Бу турдаги ҳужумлар махфий маълумотларга ёки тизимларга кириш учун инсонларни манипуляция қилишга қаратилади. Хакерлар телефон қўнғироқлари, мессенжерлардаги хабарлар, ҳатто шахсий учрашувлар орқали ҳаракат қилишлари мумкин;

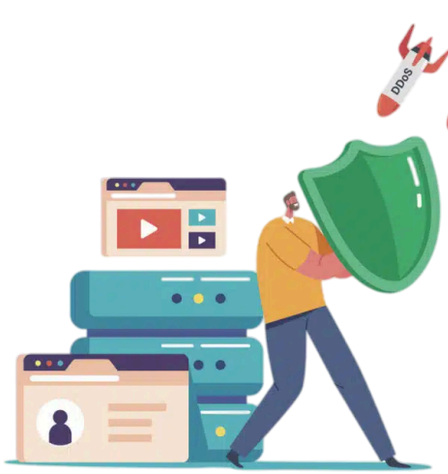
Зарарли дастур (Malware)

Бундай дастурлар маълумотларни ўғирлаш, тизимга зарар етказиш ёки компютер ресурсларини яширин бошқариш учун фойдаланувчилар қурилмаларига ўрнатилади. Улар турли шаклларда бўлиши мумкин, масалан: вируслар, троянлар, шпион дастурлар (spyware) ва бошқалар.

2 Фишингни асосий турлари

Классик фишинг

Оммавий электрон почталар юбориш, нуфузли ташкилотлар (банклар, ижтимоий тармоқлар, онлайн-сервислар) номидан ёлғон хабарномалар юбориш орқали фойдаланувчиларни тегишли ҳаволага ўтган ҳолда, сохта сайтда шахсий маълумотларини киритишга ундаш



Фарминг

Фарминг – бу фишингнинг бир тури бўлиб, унда хакерлар фойдаланувчилар трафигини расмий сайтлардан сохта саҳифаларга йўналтиради. Бунда фойдаланувчилар ўзларини тўғри сайтда деб ўйлаб, маълумотларини киритади

Қандай ҳимояланиш керак: *Шубҳали ҳаволаларни босманг – сайтнинг URL-манзилни ўзингиз мустақил равишда интернет браузерга киритинг. Икки факторли аутентификациядан (2FA) фойдаланинг – бу сизининг аккаунтларингизни пароллар ўғирланган тақдирда ҳимоя қилади.*

Мақсадли фишинг

У аниқ шахсларга қаратилган ва уларнинг иши ва ижтимоий ҳаётини ўрганиш давомида тўпланган маълумотлардан фойдаланади. Ушбу ҳужумлар жуда мослашувчан ва самарали бўлади

Вишинг (Vishing)

Бу телефон орқали амалга ошириладиган фишинг тури бўлиб, унда ҳужумчилар фойдаланувчиларни конфиденциал маълумотларини ошкор қилишга ва ишонтиришга ҳаракат қиладилар

Смишинг (Smishing)

SMS хабар орқали амалга ошириладиган фишинг, хабарда зарарли сайтга ҳавола ёки шахсий маълумотларни бериш тўғрисида сўров мавжуд бўлади

Интернетда фишинг ҳужумлар ҳақида

3 Зарарли дастурий таъминот

Зарарли дастурий таъминот – бу дастурий таъминот бўлиб, қурилма, хизмат ёки локал тармоққа зарар етказиш ёки ундан фойдаланиш учун мўлжалланган зарарли дастур.

Кибержиноятчилар одатда маълум бир маълумотлар (электрон почта ва SMS хабарлари, пароль, логин, банк карта рақамлари ва бошқалар)га эга бўлиши ҳамда шахслардан молиявий фойда олиш учун ушбу дастурлардан фойдаланадилар

Зарарли дастурий таъминотнинг асосий турлари

Вируслар

Бу зарарли дастурий таъминотнинг энг эски турларидан бири бўлиб, у бошқа дастурлар ёки файлларга бириктирилади ва зарарланган файллар ёки дастурлар орқали тарқалади

Шпион дастурлар (Spyware)

Бу фойдаланувчи устидан кузатув олиб бориш мақсадида ишлаб чиқилган дастурий таъминот. Ушбу дастурлар фойдаланувчи томонидан қайси сайтларга ташриф қилингани ва файллар очилгани ҳақида маълумот тўплаши ҳамда пароль ва маълумотларни қўлга киритиш

Троян дастурлар (Троянлар)

Троянлар оддий дастур кўринишида бўлиши мумкин, бироқ, улар ўрнатилгандан сўнг зарарли ҳаракатлар амалга оширилади (масалан: маълумотларни ўғирлаш, масофавий кириш учун имконият яратиш ва фойдаланувчини ҳаракатларини кузатиш)

Зарарли дастурлардан қандай ҳимояланиш мумкин

Антивирус дастурий таъминоти – Ишончли антивирус дастурларидан фойдаланиб, тизимни доимий равишда сканер қилинг ва зарарли иловаларни ўчириб ташланг

Тизим янгиланишлари – Операцион тизим ва дастурларни мунтазам равишда янгилаб туриш лозим, бунда ҳужумчилар фойдаланиши мумкин бўлган заифликлардан ҳимоя қилишга ёрдам беради

Маълумотларни захира нусхасини – Маълумотларни мунтазам равишда ташқи воситаларга захира нусхасини яратиш зарур, бу келажакда ўчирилган ёки зарарланган файларни тиклашга ёрдам беради

Юклаб олишда эҳтиёт бўлинг – Файлларни фақат тасдиқланган манбалардан юклаб олинг, шубҳали ҳаволалар ва/ёки электрон хатларда илова қилинган файллардан эҳтиёт бўлинг

ЎЗБ

4 Маълумотларни чиқиб кетиши

Бу шахсга доир маълумотлар, молиявий маълумотлар, интеллектуал мулк ёки ташкилот сирлари каби конфиденциал маълумотларни рухсатсиз ошкор қилиш ёки узатишдир. Бунда маълумотларни чиқиб кетиши хакерларнинг ҳаракатлари, масъул ходимларнинг эҳтиётсизлиги (инсон омили) сабабли содир бўлиши мумкин

ЎЗБ

Эълонлар тахтасида фирибгарлик

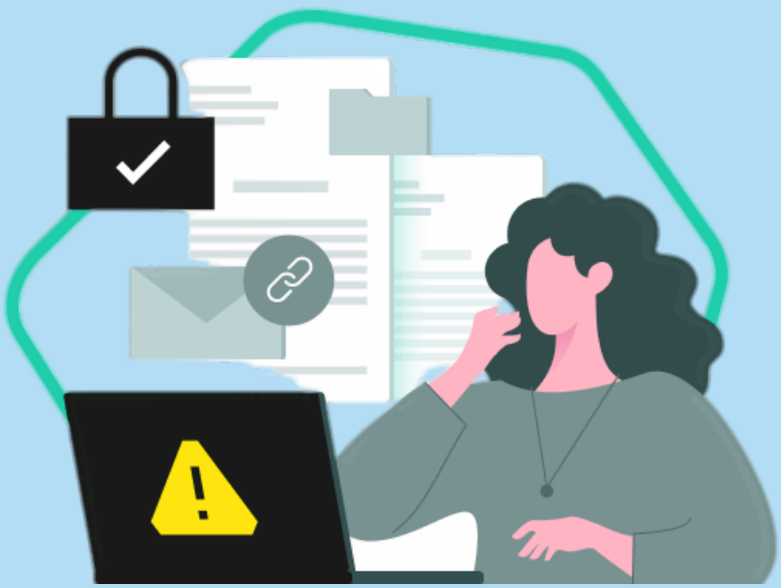

Маълумотларни чиқиб кетишининг асосий сабаблари
Конфиденциал маълумотларни сақлайдиган ноутбуклар, смартфонлар ёки ташқи хотира қурилмаларининг йўқолиши ёки ўғирланиши
Қурилма ёки маълумот сақлаш воситалари утилизация ёки бошқа шахсларга топширишдан аввал тўғри тозаланмаса, тегишли маълумотлар тасодифан ошкор бўлиши мумкин
Маънавий эскирган ёки ҳимояланмаган дастурий таъминотлардан фойдаланиш, хакерларнинг заифликлар орқали маълумотларга кириш имкониятини яратиши
Тегишли хавфсизлик чораларининг йўқлиги, жумладан шифрлаш, мураккаб пароль ва икки факторли аутентификация
Маълумотлар базаларини бузилиши, дастурий таъминот ёки тармоқлар заифликларидан фойдаланиш, фишинг ҳамда бошқа кибержиноятчилар усуллари
Инсон омили, конфиденциал маълумотларга эга ходимлар ёки ташкилот ҳамкорларининг эътиборсизлиги

1. Рискларни минималлаштириш

2. Малака ва хабардорликни ошириш

3. Шахсга доир маълумотларни ҳимоя қилиш

4. Замонавий таҳдидлар – Deepfake ва сунъий интеллект (СИ)



1 Рискларни минималлаштириш

Бу кибертаҳдидлар эҳтимолини камайтириш ва улар амалга оширилган тақдирда мумкин бўлган зарарни минималлаштиришга қаратилган комплекс тадбирлар мажмуи. Рақамли гигиена принциплари маълумотлар ва тизимларни ташқи ва ички таҳдидлардан ҳимоя қилишда асосий ўрин тутади

Ахборот тизимлари ва маълумотларни ҳимоя қилиш ҳамда тегишли чораларни кўриш ташқи ва ички ҳужумлар эҳтимолини сезиларли даражада камайтиради. Рискларни тўлиқ бартараф этиш мумкин бўлмаса-да, рақамли гигиена принциплари уларни минимал даражага келтириш ва юзага келиши мумкин бўлган оқибатларни камайтиришга имконият беради

2 Малака ва хабардорликни ошириш

Бу кибертаҳдидлардан маълумот ва тизимларни ҳимоя қилиш стратегиясининг муҳим элементлари ҳисобланади. Агар ташкилот масъул ходимлари таҳдидларни тушунмасалар ва иш жараёнида хавфсизлик қоидаларига риоя қилмасалар, ҳатто энг замонавий технологиялар ҳам уларнинг хавфсизлигини таъминлай олмайди. Ўқув дастурларини ташкил этиш орқали жамоада хавфсизлик маданияти шаклланади, бунда ҳар бир ходимга маълумотларни ҳимоя қилишдаги роли белгилаб берилади

Малака ва хабардорликни ошириш усуллари:	
Семинар ва тренинглар	Машғулот ва амалий тренинглар масъул ходимларга таҳдидларни чуқурроқ тушунишга ва ҳимоя усулларини ўзлаштиришга ёрдам беради. Бунда, ходимлар ўз фаолиятида дуч келиши мумкин бўлган реал ҳолатларга алоҳида эътибор қаратилади
Ҳақиқий ҳужумларни имитация қилиш	Ташкилот ходимлари учун фишинг-ҳужумлар, вируслар билан зарарланиш ёки бузиб кириш ҳолатларини симуляция тадбирлари ўтказилади
Билимларни синовдан ўтказиш	Ҳодимларнинг даврий синовдан ўтказилиши уларнинг билим даражасини баҳолаш ва қўшимча малака оширишга талаб мавжудлиги аниқланади
Эслатма ва йўриқномалар	Эслатмалар, йўриқномалар ва маълумотлар билан хавфсиз ишлаш бўйича қўлланмаларини ишлаб чиқиш ҳамда доимий равишда ходимларни таништириш, ахборот хавфсизлигини асосий қоидаларини мустаҳкамлашга ёрдам беради

3 Шахсга доир маълумотларни ҳимоя қилиш

Шахсга доир маълумотларни ҳимоя қилиш ахборот хавфсизлигининг асосий талабларидан бири бўлиб, у шахсий маълумотларга рухсатсиз кириш, маълумотларнинг ошкор қилиниши ёки ноқонуний фойдаланилишининг олдини олишга йўналтирилган.

Исмлар, манзиллар, телефон рақамлари, банк реквизитлари, паспорт ва ID карталар каби шахсий маълумотлар кибер жиноятчилар учун муҳим аҳамиятга эга

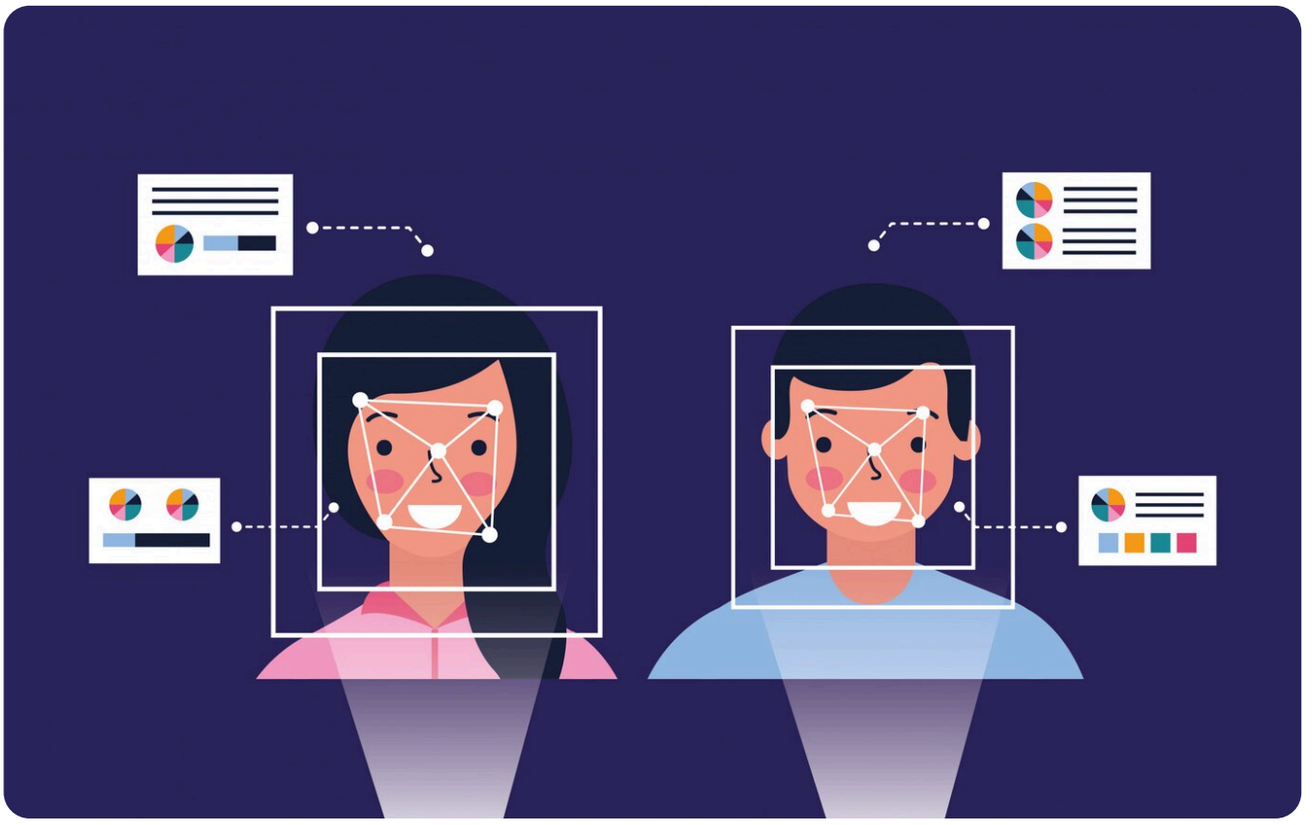
Шахсий маълумотларни ҳимоя қилиш бўйича асосий тавсиялар

1. Шахсга доир маълумотларни тақдим этишда эҳтиёт бўлиш
2. Шахсга доир маълумотларни тақдим этиш минимал даражада бўлиши ва фақат зарур ҳолларда амалга ошириш
3. Бир хил паролдан бир нечта сервисларда фойдаланмаслик
4. Жамоат Wi-Fi тармоқларида ишлашда эҳтиёт бўлиш
5. Мобил иловаларни ўрнатишдан олдин, унинг махфийлик сиёсати билан танишиш

ЎЗБ

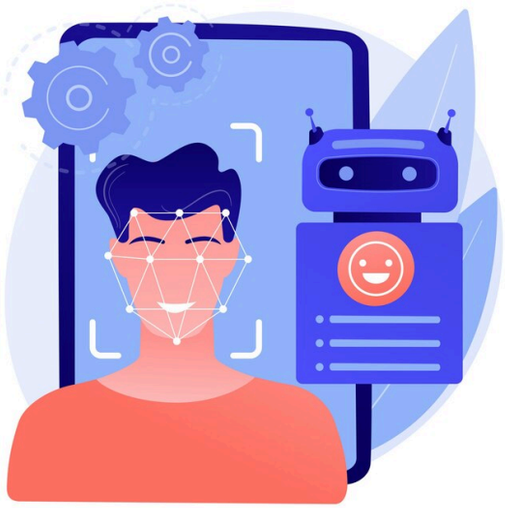
4 Замонавий таҳдидлар – Deepfake ва сунъий интеллект (СИ)

Deepfake (инглизча deep learning — чуқур ўрганиш ва fake - сохта) - сунъий интеллект (AI) ёрдамида реал кўринишдаги сохта тасвирлар, видео ва аудиоларни яратиш имконини берувчи замонавий технология. Шунингдек, мазкур усул чуқур ўрганиш алгоритмларидан фойдаланишга асосланган бўлиб, унда катта ҳажмдаги маълумотлар ўқитилади ва инсоннинг ташқи кўриниши, овози ёки хатти-ҳаракатларини қайта яратиш ҳамда сохталаштириш имконини беради



4 Замонавий таҳдидлар – Deepfake ва сунъий интеллект (СИ)

Давлат хизматчилари томонидан “Deepfake”дан фойдаланиш хавфлари:



Реал кўринишдаги сохта видеолар яратиш орқали давлат хизматчиларини ноқонуний ёки ахлоқсиз ҳаракатларни содир этаётгандай кўрсатиш

“Deepfake” давлат раҳбарлари номидан ёлғон баёнотлар яратиш учун қўлланилиши мумкин, бу эса жамиятда саросима ёки дипломатик можаролар каби инқирозларга олиб келиши мумкин

“Deepfake” - аудио раҳбарнинг овозини тақлид қилиб, ходимларни алдаш ва махфий маълумотларга кириш учун фойдаланилиши мумкин

4 Замонавий таҳдидлар – Deepfake ва сунъий интеллект (СИ)

”Deepfake” технологиясидан ҳимояланиш усуллари:

1

“Deepfake” ҳолатларни аниқлаш учун тегишли технологияларидан фойдаланиш:

- Сохта контентни таҳлил қилиш учун дастурлар ва алгоритмлардан фойдаланиш (масалан, Microsoft Video Authenticator, Deepware Scanner).
- Асл нусҳаларнинг ҳақиқийлигини текшириш учун хавфсиз белгиларини жорий этиш технологиялари

2

Рақамли гигиенани таъминлаш:

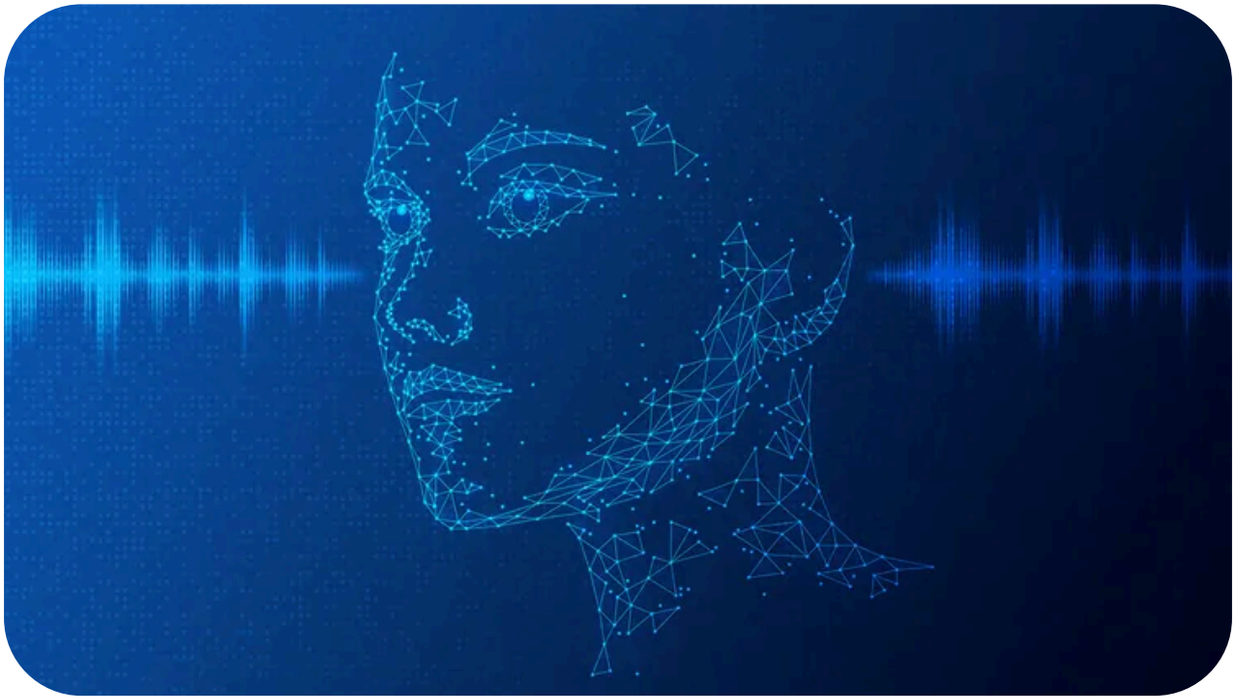
- Шахсий маълумотлар ва контент (фото, видео)нинг чоп этилишини минималлаштириш, чунки улар дипфейк яратишда ишлатилиши мумкин.
- Шубҳали материалларни тарқатишдан олдин уларнинг ишончлилигини текшириш

3

Малака ва хабардорликни ошириш:

- Давлат хизматчиларини ушбу соҳада билим ва кўникмасини ошириш;
- "Deepfake" ёрдамида ҳужумлар симуляциясини ўтказиш орқали мунтазам малкани ошириб бориш

4 Замонавий таҳдидлар – Deepfake ва сунъий интеллект (СИ)



“Deepfake” ва бошқа сунъий интеллектга асосланган технологиялар замонавий рақамли дунёда ҳақиқий таҳдидни келтириб чиқаради. Ушбу таҳдидларга қарши курашиш учун комплекс ёндашув зарур: технологиялардан фойдаланиш, ходимлар билимларини ошириш ва ҳуқуқий чораларни жорий этиш.

Бу, ўз навбатида, давлат хизматчиларига ўз обрўси ва жамоат манфаатларини ҳимоя қилишга имкон беради

ЎЗБ

Рақамли гигиена – кибертаҳдидларнинг олдини олиш учун киберхавфсизликка оид фойдали кўникмаларни шакллантириш ва ривожлантириш

кибермакон – ахборот технологиялари ёрдамида яратилган виртуал муҳит

кибертаҳдид – кибермаконда шахс, жамият ва давлат манфаатларига таҳдид солувчи шарт-шароитлар ва омиллар мажмуи

киберхавфсизлик – кибермаконда шахс, жамият ва давлат манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати

киберҳужум – кибермаконда аппарат, аппарат-дастурий ва дастурий воситалардан фойдаланган ҳолда қасддан амалга ошириладиган, киберхавфсизликка таҳдид соладиган ҳаракат

фишинг – конфиденциал маълумотларни қўлга киритиш учун фирибгарлик йўли билан амалга оширилган киберхуруж

зарарли дастур (Malware) – тизимга зарар етказиш ёки маълумотларни ўчириш ва олиш учун мўлжалланган дастурлар

DDoS-ҳужум – сервер ёки тармоқни юкламасини сунъий ошириш орқали уларни ишдан чиқаришга қаратилган ҳужум

икки факторли аутентификация (2FA) – ҳимоя қилиш учун қўшимча хавфсизлик даражаси

маълумотларни захиралаш – маълумотларни йўқолишидан ҳимоя қилиш учун уларнинг нусхаларини яратиш

шахсга доир маълумотлар – муайян жисмоний шахсга тааллуқли бўлган ёки уни идентификация қилиш имконини берадиган, электрон тарзда, қоғозда ва (ёки) бошқа моддий жисмда қайд этилган ахборот

учинчи шахс – субъект, мулкдор ва (ёки) оператор бўлмаган, аммо шахсга доир маълумотларга ишлов бериш бўйича ҳолатлар ёки муносабатлар орқали улар билан боғлиқ бўлган ҳар қандай шахс

давлат фуқаролик хизмати – давлат хизматининг бир тури бўлиб, Ўзбекистон Республикаси фуқароларининг давлат фуқаролик хизмати лавозимларидаги давлат органлари ваколатлари амалга оширилишини таъминлашга доир ҳақ тўланадиган касбий фаолиятини ифодалайди

рискларни минималлаштириш – таҳдидлар ва уларнинг оқибатларини камайтиришга қаратилган амалий чоралар

антивирус дастурий таъминоти – зарарли дастурларни аниқлаш, блоклаш ва ўчириш учун мўлжалланган дастур

фарминг – фойдаланувчиларни қонуний сайтлардан сохта саҳифаларга йўналтириш

вишинг (Vishing) – телефон орқали амалга ошириладиган фишинг ҳужумлар

смишинг (Smishing) – матнли хабарлар (SMS) орқали амалга ошириладиган фишинг ҳужумлар

мураккаб пароллар – хавфсизлик даражасини ошириш учун ўзига хос пароллар

Норматив-ҳуқуқий ҳужжатлар

Ўзбекистон Республикасининг “Давлат фуқаролик хизмати тўғрисида”ги

ЎРҚ-788-сон Қонуни

Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги

ЎРҚ-764-сон Қонуни

Ўзбекистон Республикасининг “Шахсга доир маълумотлар тўғрисида”ги

ЎРҚ-547-сон Қонуни

АГЕНТСТВО РАЗВИТИЯ
ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ
РЕСПУБЛИКИ УЗБЕКИСТАН

CYBER SECURITY CENTER

ЦИФРОВАЯ ГИГИЕНА

информационная безопасность в киберпространстве

СОДЕРЖАНИЕ

РУС

Цифровая гигиена — это не просто набор рекомендаций, а неотъемлемая часть современной жизни, требующая постоянного внимания и действий. Соблюдение принципов цифровой гигиены защищает личные данные, предотвращает кибератаки и способствует созданию безопасной онлайн-среды в киберпространстве. Важно, чтобы как индивидуальные пользователи, так и организации понимали значимость цифровой гигиены и регулярно обновляли свои знания и навыки в этой области

ЧАСТЬ 01

Введение

1. Понятие цифровой гигиены

2. Важность цифровой гигиены для госслужащих

3. Основные рекомендации для госслужащих

РУС

1 Понятие цифровой гигиены

Цифровая гигиена

Это формирование полезных привычек в отношении кибербезопасности, позволяющих не стать жертвой киберугроз и избегать проблем сетевой безопасности. Цифровая гигиена иногда сравнивают с личной гигиеной: в обоих случаях это регулярные меры для обеспечения здоровья и благополучия

Ключевые аспекты цифровой гигиены

Безопасное управление паролями:

Использование сложных, уникальных паролей для разных учетных записей и регулярная их смена являются основой цифровой безопасности

Обновление программного обеспечения:

Регулярное обновление операционных систем и приложений позволяет закрыть уязвимости, которые могут быть использованы злоумышленниками

1 Понятие цифровой гигиены

Двухфакторная аутентификация (2FA)

Включение двухфакторной аутентификации добавляет дополнительный уровень безопасности, требуя не только пароль, но и второй способ подтверждения личности

Использование антивирусных программ и фаерволов

Антивирусное ПО помогает обнаруживать и предотвращать угрозы, такие как вирусы, трояны и шпионские программы, а фаерволы ограничивают доступ к компьютеру извне

Безопасность Wi-Fi

Обеспечение защиты сети Wi-Fi с помощью сложных паролей и шифрования помогает предотвратить несанкционированный доступ к сети

Защита личной информации:

Госслужащие должны осознанно подходить к размещению информации в социальных сетях и на открытых ресурсах. Важно настраивать параметры конфиденциальности, чтобы ограничить доступ к личным данным

Распознавание угроз:

Знание о кибербезопасности и других формах социальной инженерии позволяет госслужащим более эффективно защищаться от атак

Подозрительные ссылки и вложения:

Избегание перехода по сомнительным ссылкам и открытия подозрительных вложений в электронной почте для защиты от фишинговых атак и вредоносных программ

Основные аспекты цифровой гигиены

Цифровая гигиена помогает не только защитить личные данные, но и обеспечивает более безопасное и ответственное использование технологий в повседневной жизни

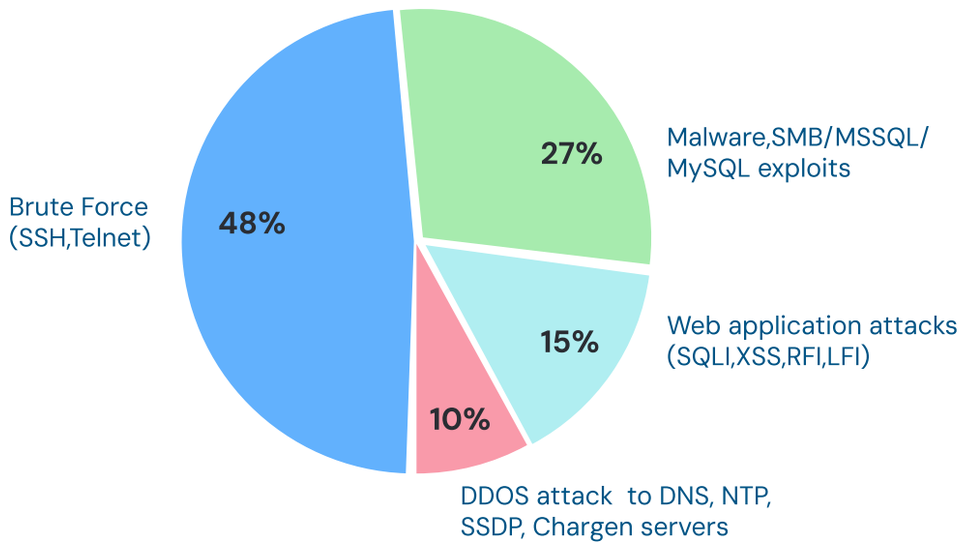
2 Важность цифровой гигиены для госслужащих

Цифровая гигиена для госслужащих является критически важной, поскольку сотрудники государственных учреждений имеют доступ к чувствительной информации, которая может быть использована не только для обеспечения функционирования государства, но и для принятия стратегических решений. Несоблюдение принципов цифровой безопасности может привести к утечке личных данных, государственным утратам и серьезным киберугрозам

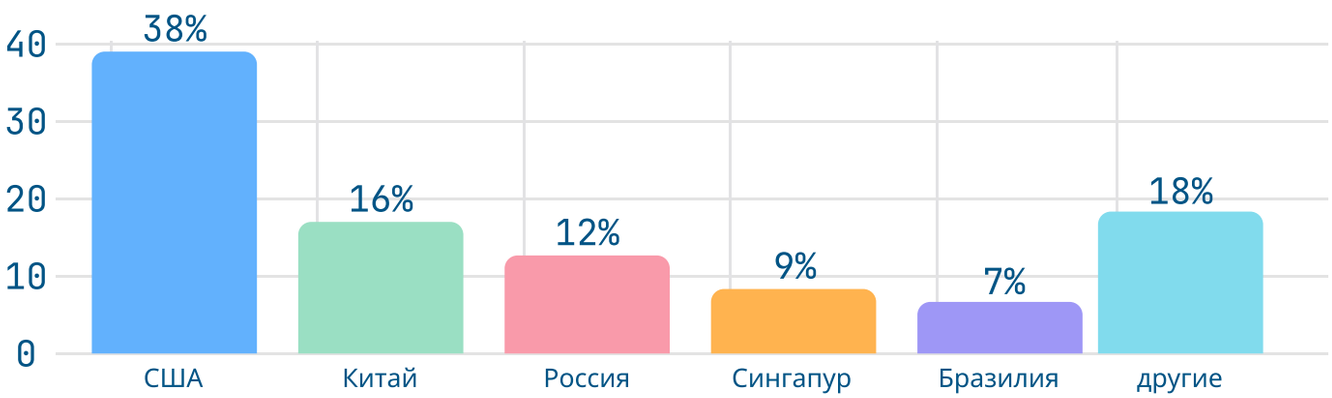
Кибератаки, зафиксированные в домене “uz”

В течение 2024 года на системы "Honeypot*" было совершено более 70 миллионов кибератак

Наиболее распространённые виды атак



Кибератаки в разрезе стран



*Honeypot – ресурс, представляющий собой приманку для злоумышленников чтобы изучить их стратегию и определить перечень средств, с помощью которых могут быть нанесены удары по реально существующим объектам безопасности.

2 Важность цифровой гигиены для госслужащих

Важность цифровой гигиены для госслужащих

Защита конфиденциальной информации:

Государственные служащие повышают навыки соблюдения правил информационной безопасности при использовании персональных данных, государственных и финансовых тайн, а также другой конфиденциальной информации

Устойчивость к инцидентам безопасности:

Правильные практики цифровой гигиены способствуют быстрому реагированию на инциденты, что может значительно уменьшить их последствия

Сохранение репутации государственных органов:

Нарушение цифровой безопасности может подорвать доверие граждан к государственным учреждениям. Соблюдение цифровой гигиены демонстрирует ответственное отношение к своим обязанностям

Повышение цифровой грамотности:

Постоянное обучение в области кибербезопасности и цифровой гигиены позволяет госслужащим оставаться в курсе новых угроз и технологий

Предотвращение кибератак:

Современные угрозы, такие как фишинг, вредоносные программы и взломы, требуют осведомленности и навыков в области кибербезопасности. Использование сложных паролей, двуфакторной аутентификации и обновленного программного обеспечения снижает риски

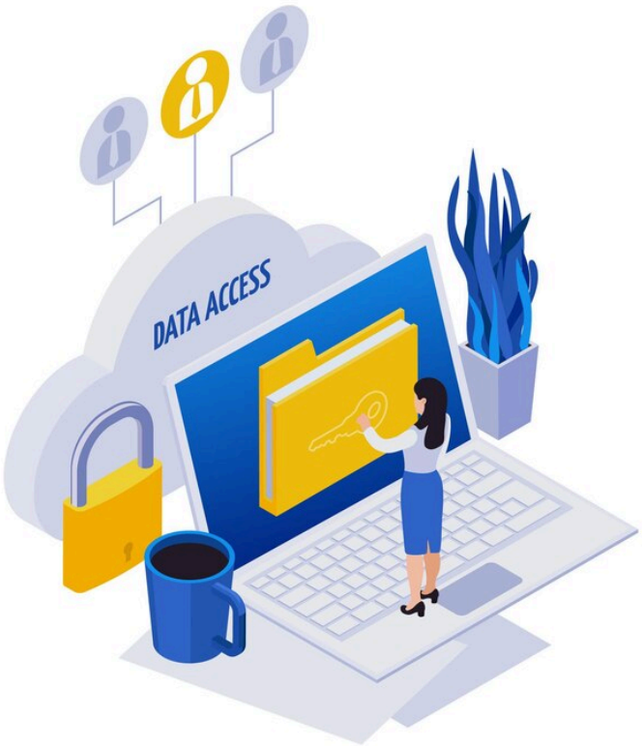
2 Основные рекомендации для государственных служащих

В процессе выполнения своих функциональных обязанностей строго соблюдать правила и порядок, установленные в «Политике информационной безопасности»

При работе с информационными системами и ресурсами не разглашать третьим лицам, включая представителей других организаций и предприятий, данные о своем логине, пароле (в том числе данные Единой системы идентификации - ONE ID), электронной цифровой подписи (ЭЦП), номерах банковских карт, а также подтверждающие коды, полученные через SMS, и другие подобные сведения

РУС

Если мошенник звонит, не поддавайтесь на обман!



В организации следует незамедлительно информировать ответственное подразделение в указанных случаях для обеспечения информационной безопасности:

- о необоснованном разглашении информации и сотрудниках, допустивших это;
- об организациях или третьих лицах, проявивших интерес к информации и пытавшихся её получить;
- о фактах утраты документов, содержащих конфиденциальную информацию, в бумажной или электронной форме;
- о размещение конфиденциальной информации на интернет-сайтах, форумах, в социальных сетях;
- об оставление конфиденциальных документов в открытых местах (на принтере, в переговорной комнате) и другие случаи.

ЧАСТЬ 02

Основные аспекты цифровой гигиены

1. Кибератаки

2. Основные виды фишинга

3. Вредоносное ПО

4. Утечка данных

РУС

1 Кибератаки

Действие, представляющее угрозу кибербезопасности, умышленно осуществляемое в киберпространстве с использованием аппаратных, аппаратно-программных и программных средств.

Кибератаки могут варьироваться от простых до крайне сложных и включают в себя множество различных методов, таких как фишинг, взлом паролей, внедрение вредоносного программного обеспечения (вирусы, трояны, шпионское ПО), атаки типа "отказ в обслуживании" (DDoS)и т.д.

Основные виды кибератак:

Фишинг

Это метод кражи конфиденциальных данных через обман. Пользователям отправляются поддельные сообщения (например, письма, похожие на официальные уведомления от банка или другой организации), которые заставляют их раскрыть личную информацию или перейти по вредоносной ссылке;

Будьте бдительны! Распространяется новый вид мошенничества

1 Кибератаки

Атаки (Man in the Middle)

При таких атаках злоумышленник перехватывает и изменяет коммуникацию между пользователем и сервером, часто без ведома жертвы. Это может происходить через незащищенные сети Wi-Fi или другие уязвимости;

SQL-инъекции

Атаки на базы данных, когда злоумышленники используют уязвимости в коде веб-приложений, чтобы вставить вредоносный код, который может раскрыть или изменить информацию в базе данных;

DDoS-атаки

Такие атаки направлены на перегрузку серверов или сетевой инфраструктуры с помощью большого объема трафика, что приводит к сбоям в работе сайтов или сервисов;

Брутфорс

Это метод перебора всех возможных комбинаций для нахождения правильного пароля или ключа шифрования. Этот подход применяется злоумышленниками для взлома защищённых аккаунтов, систем или зашифрованных данных, когда другие методы, такие как фишинг или социальная инженерия, не сработали;

Социальная инженерия

Этот тип атак направлен на манипулирование людьми для получения доступа к конфиденциальной информации или системам. Злоумышленники могут действовать через телефонные звонки, сообщения в мессенджерах или даже личные встречи;

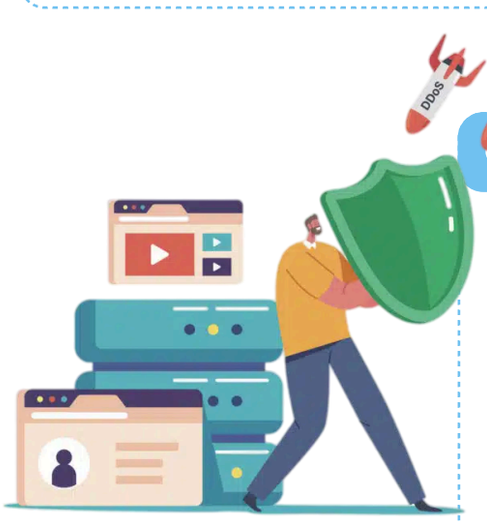
Вредоносное ПО(Malware)

Программы, которые внедряются на устройства жертв для кражи данных, повреждения системы или скрытого управления ресурсами компьютера. Это могут быть вирусы, трояны, программы-вымогатели и т.д..

2 Основные виды фишинга

Классический фишинг

Отправка массовых электронных писем, поддельных уведомлений от известных организаций (банков, социальных сетей, онлайн-сервисов), побуждающих пользователя перейти по ссылке и ввести личные данные на поддельном сайте



Фарминг

Это тип фишинга, при котором злоумышленники перенаправляют трафик пользователей с легитимных сайтов на поддельные страницы, где они вводят свои данные, думая, что находятся на правильном сайте

Как защититься: *Не кликайте на подозрительные ссылки — вместо этого посетите сайт вручную, вводя URL в браузере. Используйте двухфакторную аутентификацию (2FA) — это защитит ваши аккаунты даже в случае, если ваши пароли будут украдены.*

Целенаправленный

Атаки, направленные на конкретного человека или организацию. Злоумышленники изучают информацию о жертве, чтобы создать персонализированное сообщение которое выглядит убедительно и вызывает доверие

Вишинг (Vishing)

Разновидность фишинга через телефонные звонки, когда злоумышленники пытаются убедить жертву передать им конфиденциальную информацию

Смишинг (Smishing)

Фишинг с использованием SMS, когда в сообщении содержится ссылка на вредоносный сайт или просьба передать личные данные

Что такое фишинг и фишинговая атака

2 Вредоносное ПО

Вредоносная программа – это программное обеспечение, предназначенное для нанесения вреда устройству, сервису или локальной сети либо для их несанкционированного использования.

Киберпреступники обычно используют такие программы, чтобы получить доступ к определённым данным (электронная почта и SMS-сообщения, пароли, логины, номера банковских карт и другие сведения) и извлечь финансовую выгоду за счёт пользователей

Основные типы вредоносного ПО

Вирусы

Это один из старейших видов вредоносного ПО, который присоединяется к другим программам или файлам и распространяется через заражённые файлы или программы

Шпионские программы (Spyware)

Это ПО, которое устанавливается на устройство с целью шпионажа за пользователем Шпионское ПО может собирать информацию о том, какие сайты посещает пользователь, какие файлы открывает, и даже перехватывать пароли и другую конфиденциальную информацию

Троянские программы (Трояны)

Трояны маскируются под легитимные программы, но, после их установки, могут выполнять вредоносные действия, такие как кража данных, открытие "задних дверей" для удалённого доступа или шпионаж за пользователем

Антивирусное программное обеспечение — Используйте надёжные антивирусные программы для регулярного сканирования системы и удаления вредоносных приложений

Обновления системы — Регулярно обновляйте операционную систему и программы для защиты от уязвимостей, которые могут использовать злоумышленники

Резервное копирование данных — Регулярное резервное копирование данных на внешние носители или в облако поможет восстановить файлы в случае атаки вымогателей

Осторожность при загрузках — Загружайте файлы только из проверенных источников, избегайте подозрительных ссылок и вложений в электронных письмах

4 Утечка данных

Это несанкционированное раскрытие или передача конфиденциальной информации, такой как личные данные, финансовая информация, интеллектуальная собственность или корпоративные секреты. Утечка может произойти как в результате злонамеренных действий злоумышленников (хакеров), так и по вине сотрудников организаций из-за неосторожности или человеческой ошибки

РУС

Мошенничество на досках объявлений

Данные могут быть случайно раскрыты, если устройства или носители информации не были надлежащим образом очищены перед утилизацией или передачей

Физическая потеря или кража ноутбуков, смартфонов или внешних накопителей, содержащих конфиденциальную информацию, может стать причиной утечки данных

Использование устаревшего или незащищённого программного обеспечения может привести к тому, что хакеры смогут получить доступ к данным через уязвимости

Основные причины утечки данных

Отсутствие адекватных мер безопасности, таких как шифрование, сложные пароли или двухфакторная аутентификация, может сделать данные уязвимыми для утечек

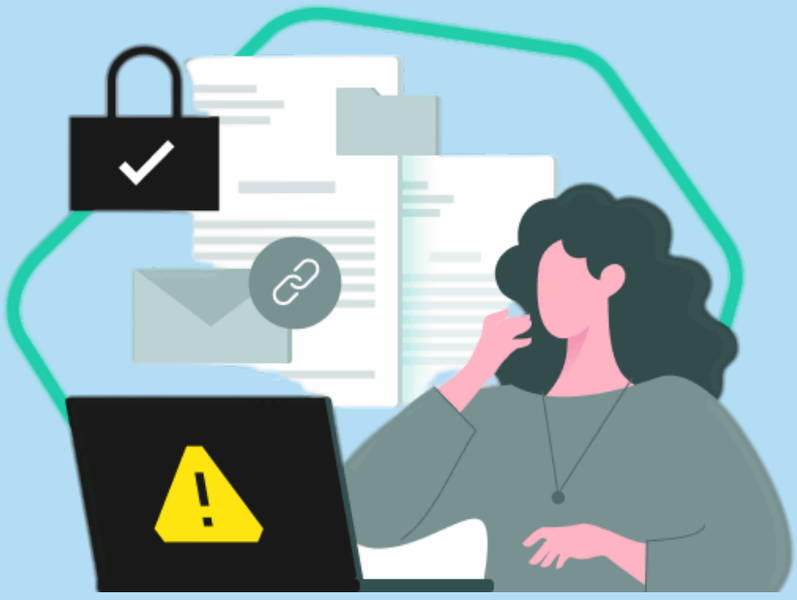
Взломы баз данных, использование уязвимостей программного обеспечения или сетей, фишинг и другие методы киберпреступников могут привести к утечке данных

Утечки могут происходить из-за действий сотрудников или партнёров организации,которые имеют доступ к конфиденциальной информации.

ЧАСТЬ 03

Принципы цифровой гигиены ИБ

1. Минимизация рисков
2. Обучение и повышение осведомленности
3. Защита личных данных
4. Современные угрозы – Deepfake и искусственный интеллект (ИИ)



РУС

1 Минимизация рисков

Это комплекс мер, направленных на снижение вероятности возникновения угроз и уменьшение возможного ущерба в случае реализации тех или иных киберугроз. Принципы цифровой гигиены информационной безопасности играют ключевую роль в защите информации и систем от внешних и внутренних угроз

Простые и регулярные действия по защите информационных систем и данных значительно снижают вероятность успешных атак. Несмотря на то, что нельзя полностью исключить риски, принципы цифровой гигиены позволяют минимизировать их и уменьшить потенциальные последствия

2 Обучение и повышение осведомленности

Это важные элементы в стратегии защиты данных и систем от киберугроз. Даже самые современные технологии не смогут обеспечить полную безопасность, если сотрудники организации не понимают возможных угроз и не умеют применять безопасные практики в повседневной работе. Внедрение программ обучения позволяет создать культуру безопасности, где каждый сотрудник осознает свою роль в защите корпоративной информации

Методы обучения и повышения осведомлённости:

Семинары и тренинги	Очные занятия и практические тренинги помогают участникам глубже понять угрозы и освоить методы защиты. Особое внимание уделяется реальным сценариям, с которыми могут столкнуться сотрудники в своей работе
Имитация реальных атак	Организация может проводить регулярные симуляции фишинг-атак, вирусных заражений или взломов для практического обучения сотрудников
Тесты на знание ИБ	Периодическое тестирование сотрудников позволяет оценить уровень их знаний и выявить пробелы, требующие дополнительного обучения
Памятки и инструкции	Создание и распространение кратких памяток, инструкций и руководств по безопасным методам работы с информацией помогает закрепить основные правила информационной безопасности

3 Защита личных данных

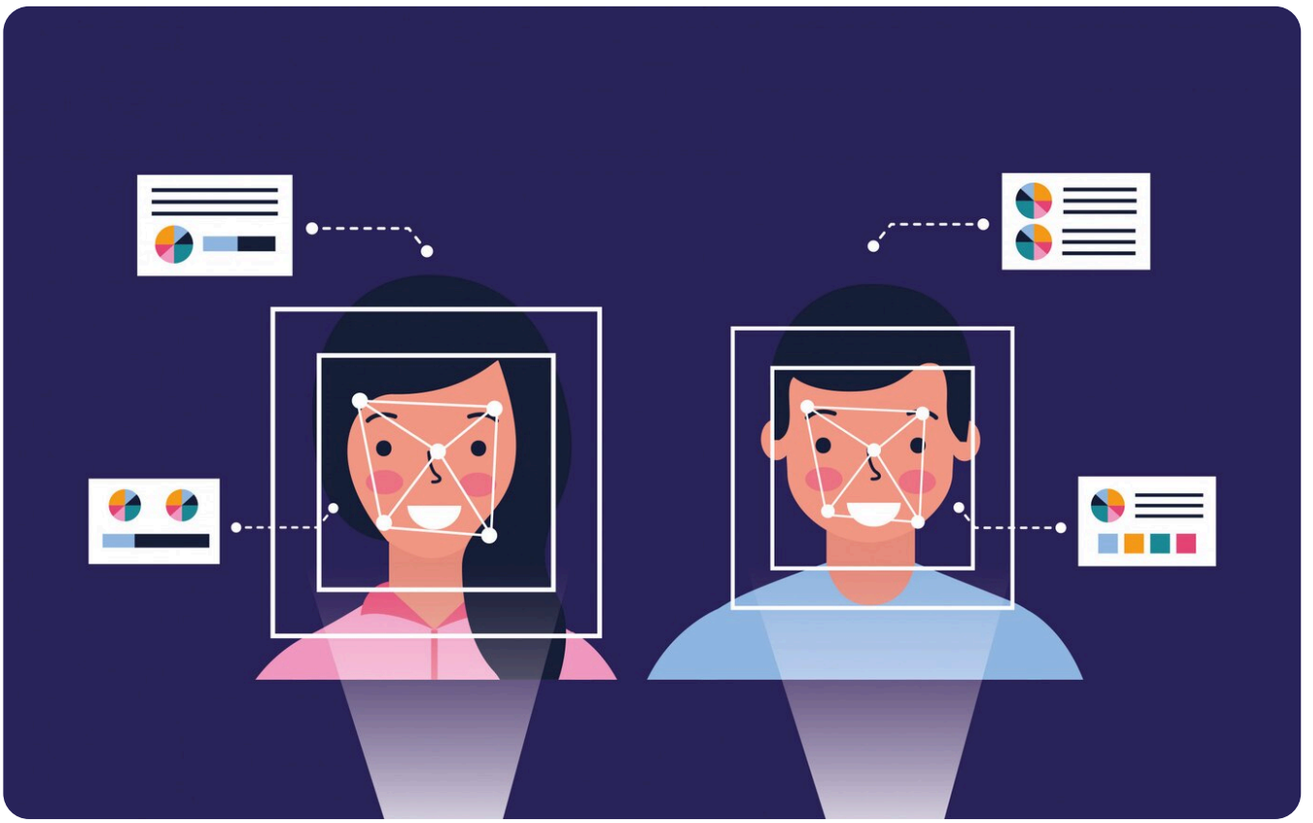
Это ключевые аспекты информационной безопасности, направленные на предотвращение несанкционированного доступа, утечки или неправомерного использования персональной информации. Личные данные, такие как имена, адреса, номера телефонов, банковские реквизиты, номера паспортов и идентификационных карт, являются ценными для кибер преступников.

Основные рекомендации по защите личных данных

1. Соблюдайте осторожность при предоставлении личных данных
2. Передача персональных данных должна быть минимальной и происходить только в случае необходимости
3. Избегайте использования одного пароля для нескольких сервисов
4. Будьте осторожны при работе с общественными Wi-Fi сетями
5. Прежде чем установить мобильные приложения, необходимо изучить их политику конфиденциальности

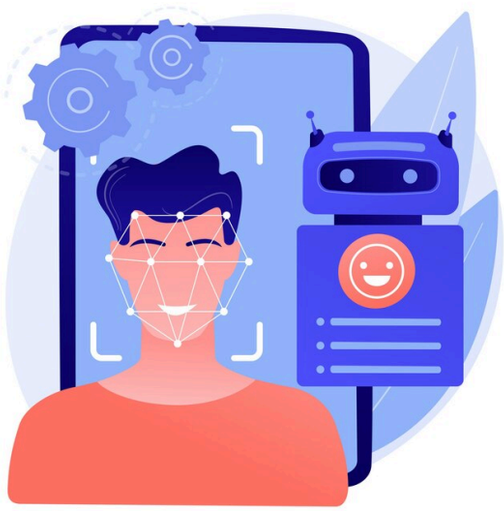
4 Современные угрозы – “Deepfake“ и искусственный интеллект (ИИ)

Deepfake (от английского deep learning — глубокое обучение и fake — подделка) — это технология, которая использует искусственный интеллект (ИИ) для создания реалистичных фальшивых изображений, видео или аудио. Этот метод основан на использовании алгоритмов глубокого обучения, которые обучаются на больших объемах данных, чтобы воспроизводить и подделывать внешность, голос или поведение человека



4 Современные угрозы – “Deepfake“ и искусственный интеллект (ИИ)

Опасности использования “Deepfake” для госслужащих:



Госслужащих могут выставить в неприглядном свете, создав фальшивое видео с их участием, где они якобы совершают незаконные или аморальные действия.

“Deepfake” может быть использован для создания ложных заявлений от имени государственных лидеров, что способно вызвать кризисы, например, панику на рынке или дипломатический скандал.

“Deepfake”-аудио может быть использовано для обмана сотрудников, имитируя голос их начальника, чтобы получить доступ к конфиденциальным данным

4 Современные угрозы – “Deepfake“ и искусственный интеллект (ИИ)

Как защититься от “Deepfake”?

1

Использование технологий для обнаружения “Deepfake”:

- Программы и алгоритмы для анализа поддельного контента (например, Microsoft Video Authenticator, Deepware Scanner)
- Внедрение технологий водяных знаков на оригинальных записях для проверки их подлинности

2

Обеспечение цифровой гигиены:

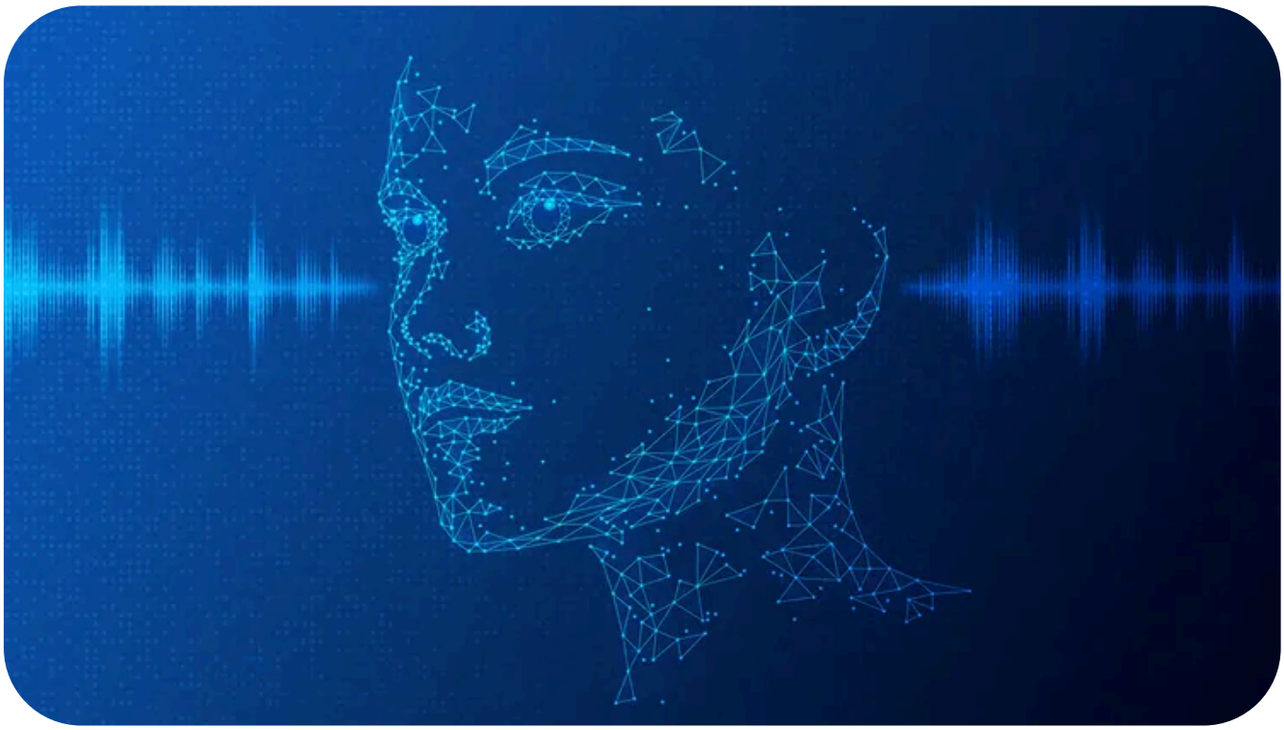
- Минимизация публикации личных данных и контента (фото, видео), которые могут быть использованы для создания “Deepfake”.
- Проверка достоверности подозрительных материалов перед их распространением

3

Обучение и повышение осведомленности:

- Обучение госслужащих навыкам распознавания поддельного контента.
- Регулярные тренировки, включая симуляции атак с использованием “Deepfake”

4 Современные угрозы – “Deepfake“ и искусственный интеллект (ИИ)



“Deepfake” и другие технологии, основанные на искусственном интеллекте, представляют реальную угрозу в современном цифровом мире. Борьба с этими угрозами требует комплексного подхода: использования технологий, повышения уровня знаний сотрудников.

Для госслужащих особенно важно защитить свою репутацию и государственные интересы.

Появился новый вид мошенничества с использованием искусственного интеллекта.

ЧАСТЬ 04

Термины и определение

Цифровая гигиена – формирование и развитие полезных навыков в отношении кибербезопасности для предотвращения киберугроз

киберпространство – виртуальная среда, созданная с помощью информационных технологий

киберугроза – комплекс условий и факторов в киберпространстве, представляющих угрозу интересам личности, общества и государства

кибербезопасность – состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве

кибератака – действие, представляющее угрозу кибербезопасности, умышленно осуществляемое в киберпространстве с использованием аппаратных, аппаратно-программных и программных средств

фишинг – мошенничество, связанное с попыткой обманным путем получить конфиденциальные данные

вредоносное ПО (Malware) – программы, предназначенные для нанесения ущерба системе или кражи данных

DDoS-атака – перегрузка серверов или сетей с целью их отключения

двухфакторная аутентификация (2FA) – дополнительный уровень защиты учетных записей

резервное данных – создание копий информации для защиты от потери данных

персональные данные – зафиксированная на электронном, бумажном и (или) ином материальном носителе информация, относящаяся к определенному физическому лицу или дающая возможность его идентификации

третье лицо – любое лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними обстоятельствами или отношениями по обработке персональных данных

государственная гражданская служба – вид государственной службы, представляющий собой профессиональную оплачиваемую деятельность граждан Республики Узбекистан по обеспечению осуществления полномочий государственных органов на должностях государственной гражданской службы

минимизация рисков – применение мер для уменьшения вероятности угроз и их последствий

антивирусное программное обеспечение – программы для обнаружения, блокировки и удаления вредоносного ПО

фарминг – перенаправление пользователей с легитимных сайтов на поддельные страницы

вишинг (Vishing) – фишинговые атаки, проводимые через телефонные звонки

смишинг (Smishing) – фишинговые атаки через текстовые сообщения (SMS)

сложные пароли – уникальные и трудноподбираемые пароли для повышения уровня безопасности

Нормативные правовые акты

Закон Республики Узбекистан “О государственной гражданской службе”

Закон: №ЗРУ-788

Закон Республики Узбекистан “О кибербезопасности”

Закон: №ЗРУ-764

Закон Республики Узбекистан “О персональных данных”

Закон: №ЗРУ-547

Муаллифлар: Ўзбекистон Республикаси Президенти ҳузуридаги Давлат хизматини ривожлантириш агентлиги
А.Ф. Мусаев, У.Х.Самиев, К.Гафуров, Д.Файзуллаев, Э.Равшанов

“Киберхавфсизлик маркази”
О.Н. Мирзаев, Х. Рустамов, И. Айсаев

ЮКЛАБ ОЛИНГ

Ушбу қўлланма Ўзбекистон Республикаси Президенти ҳузуридаги Давлат хизматини ривожлантириш агентлиги ҳамда Ўзбекистон Республикаси Давлат хавфсизлик хизмати ҳузуридаги “Киберхавфсизлик маркази” билан биргаликда тайёрланган

ЮКЛАБ ОЛИНГ

2025 йил