ҒТАХР 06.75.13 DOI: https://doi.org/10.62687/ESM.7.1.2025.42

БЕЛГІСІЗДІК ЖАҒДАЙЫНДА ҚАЗАҚСТАНДАҒЫ КИБЕРҚАУІПСІЗДІК АУДИТІ

[1]А.К. Алпысбаева* , **[2]Р.А. Ерниязов** , **[3]А.А. Чонкоева**
[1,2]Астана халықаралық университеті, Астана, Қазақстан
[3]И. Раззаков атындағы Қырғыз мемлекеттік техникалық университеті, Бішкек қ., Қырғызстан Республикасы
*e-mail: alpysbayeva.ainur77@mail.ru

А.К. Алпысбаева – экономика ғылымдарының кандидаты, қауым. профессоры, Астана халықаралық университеті, Астана, Қазахстан, e-mail: alpysbayeva.ainur77@mail.ru, https://orcid.org/0000-0001-6444-2148

Р.А. Ерниязов – экономика ғылымдарының кандидаты, қауым. профессоры, Астана халықаралық университеті, Астана, Қазахстан, e-mail: erniyazov$_r$$ust@mail.ru$, https://orcid.org/0009-0002-7976-6086

А.А. Чонкоева – экономика ғылымдарының кандидаты, доцент, И. Раззаков атындағы Қырғыз мемлекеттік техникалық университеті, Бішкек, Қырғызстан, e-mail: Asel.chonkoeva@kstu.kg, https://orcid.org/0009-0005-8699-9074

Аңдатпа. Мақалада Қазақстандағы киберқауіпсіздіктің қазіргі жағдайы және геосаяси, технологиялық және экономикалық факторларға байланысты өсіп келе жатқан белгісіздік жағдайында киберқауіпсіздік аудитін жүргізу ерекшеліктері қарастырылады. Зерттеу соңғы жылдардағы аналитикалық деректерге, соның ішінде киберқауіпсіздік туралы мәліметтерге, цифрландыру деңгейіне және Ұлттық киберқауіпсіздік бағдарламаларының тиімділігіне негізделген.

Қазақстанның цифрлық экожүйесін трансформациялау жағдайында ақпараттық қауіпсіздік аудитін жетілдірудің түйінді үрдістері, проблемалары мен бағыттары айқындалды. Киберқауіпсіздік кез келген заманауи бизнес стратегиясының маңызды құрамдас бөлігіне айналды, өйткені киберқылмыскерлердің қауіптері артып келеді. Киберқауіпсіздікті тексеру және бағалау ұйымдарға осалдықтарды анықтауға және олардың ақпараттық жүйелерін қорғау деңгейін анықтауға мүмкіндік береді.

Жыл сайын киберқауіптер күрделене түседі және әртүрлі болады. Шабуылдар қарапайым фишингтік схемалардан бастап зиянды бағдарламалар мен бағдарламалық жасақтаманың осалдығын пайдаланатын күрделі көп деңгейлі шабуылдарға дейін болуы мүмкін. Мұндай жағдайларда ұйымдар тек оқиғаларға жауап беруге ғана емес, сонымен қатар ықтимал қауіптерді белсенді түрде анықтауға және жоюға дайын болуы керек. Технологияның қарқынды дамуы және кибершабуылдар санының артуы жағдайында киберқауіпсіздіктің тұрақты аудиті қауіпсіз жұмысты қамтамасыз ету үшін қажетті қадамға айналады. Бұл тәуекелдерді азайтуға ғана емес, сонымен қатар клиенттер мен серіктестердің компанияға деген сенімін арттыруға мүмкіндік береді. Киберқауіпсіздікті бағалау қолданыстағы қорғаныс шараларын талдауды, сондай-ақ оларды жақсарту бойынша ұсыныстар әзірлеуді қамтиды. Осы процестің нәтижесінде компаниялар өздерінің қазіргі қауіпсіздігі туралы және анықталған кемшіліктерді жою үшін іс-қимыл жоспары туралы нақты түсінік алады.

Түйін сөздер: киберқауіпсіздік аудиті, цифрлық трансформация, тәуекел-менеджмент, цифрландыру, жасанды интеллект, белгісіздік, кибершабуылдар.

CYBERSECURITY AUDIT IN KAZAKHSTAN UNDER CONDITIONS OF UNCERTAINTY

[1]A.K. Alpysbaeva*, **[2]R.A. Yerniyazov**, **[3]A.A. Chonkoeva**
[1,2]Astana International University, Astana, Kazakhstan
[3]Kyrgyz State Technical University named after I. Razzakov, Bishkek, Kyrgyzstan
*e-mail: alpysbayeva.ainur77@mail.ru

A.K. Alpysbaev – candidate of economic sciences, associate professor, Astana International University, Astana, Kazakhstan, e-mail: alpysbayeva.ainur77@mail.ru, https://orcid.org/0000-0001-6444-2148

R.A. Yerniyazov – candidate of economic sciences, associate professor, Astana International University, Astana, Kazakhstan, e-mail: erniyazov$_{rust@mail.ru}$, https://orcid.org/0009-0002-7976-6086

A.A. Chonkoeva – candidate of economic sciences, associate professor, Kyrgyz State Technical University named after I. Razzakov, Bishkek, Kyrgyzstan, e-mail: Asel.chonkoeva@kstu.kg, https://orcid.org/0009-0005-8699-9074

Abstract. The article examines the current state of cybersecurity in Kazakhstan and the specifics of conducting a cybersecurity audit in the face of growing uncertainty caused by geopolitical, technological and economic factors. The study is based on analytical data from recent years, including information on cyber incidents, the level of digitalization, and the effectiveness of national cybersecurity programs. The key trends, problems and directions of improving information security audit in the context of the transformation of the digital ecosystem of Kazakhstan have been identified. Cybersecurity has become an important part of the strategy of any modern business, as threats from cybercriminals continue to grow. Cybersecurity audits and assessments allow organizations to identify vulnerabilities and determine the level of protection of their information systems. Cyber threats are becoming more complex and diverse every year. Attacks can range from simple phishing schemes to complex multi-layered attacks exploiting malware and software vulnerabilities. In such circumstances, organizations must be prepared not only to respond to incidents, but also to proactively identify and eliminate potential threats. With the rapid development of technology and the increasing number of cyber attacks, regular cybersecurity audits are becoming a necessary step to ensure safe operation. This allows not only to minimize risks, but also to increase the trust of customers and partners in the company. Cybersecurity assessment includes an analysis of existing security measures, as well as the development of recommendations for their improvement. As a result of this process, companies receive a clear understanding of their current security and an action plan to eliminate the identified deficiencies.

Keywords: cybersecurity audit, digital transformation, risk management, digitalization, artificial intelligence, uncertainty, cyber attacks.

АУДИТ КИБЕРБЕЗОПАСНОСТИ В КАЗАХСТАНЕ В УСЛОВИЯХ НЕОПРЕДЕЛЁННОСТИ

[1]А.К. Алпысбаева*, **[2]Р.А. Ерниязов**, **[3]А.А. Чонкоева**
[1,2]Международный университет Астана, Астана, Казахстан
[3]Кыргызский государственный технический университет им. И. Раззакова, Бишкек, Кыргызстан
*e-mail: alpysbayeva.ainur77@mail.ru

А.К. Алпысбаева – кандидат экономических наук, асс. профессор, Международный университет Астана, Астана, Казахстан, e-mail: alpysbayeva.ainur77@mail.ru, https://orcid.org/0000-0001-6444-2148

Р.А. Ерниязов – кандидат экономических наук, асс. профессор, Международный университет Астана, Астана, Казахстан, e-mail: erniyazov$_{r}ust@mail.ru$, https://orcid.org/0009-0002-7976-6086

А.А. Чонкоева – кандидат экономических наук, доцент, Кыргызский государственный технический университет им. И. Раззакова, Бишкек, Кыргызстан, e-mail: Asel.chonkoeva@kstu.kg, https://orcid.org/0009-0005-8699-9074

Аннотация. В статье рассматривается современное состояние кибербезопасности в Казахстане и особенности проведения аудита кибербезопасности в условиях растущей неопределённости, обусловленной геополитическими, технологическими и экономическими факторами. Исследование базируется на аналитических данных за последние годы, включая сведения о киберинцидентах, уровне цифровизации и эффективности национальных программ по обеспечению кибербезопасности. Определены ключевые тенденции, проблемы и направления совершенствования аудита информационной безопасности в условиях трансформации цифровой экосистемы Казахстана. Кибербезопасность стала важной составляющей стратегии любого современного бизнеса, поскольку угрозы со стороны киберпреступников продолжают расти. Аудит и оценка кибербезопасности позволяют организациям выявить уязвимости и определить уровень защиты своих информационных систем. С каждым годом киберугрозы становятся все более сложными и разнообразными. Атаки могут варьироваться от простых фишинговых схем до сложных многослойных атак, использующих вредоносное ПО и уязвимости в программном обеспечении. В таких условиях организации должны быть готовы не только к реагированию на инциденты, но и к проактивному выявлению и устранению потенциальных угроз. В условиях стремительного развития технологий и увеличения числа кибератак, регулярный аудит кибербезопасности становится необходимым шагом для обеспечения безопасной работы. Это позволяет не только минимизировать риски, но и повысить доверие клиентов и партнеров к компании. Оценка кибербезопасности включает в себя анализ существующих мер защиты, а также разработку рекомендаций по их улучшению. В результате этого процесса компании получают четкое представление о своей текущей безопасности и план действий для устранения выявленных недостатков.

Ключевые слова: аудит кибербезопасности, цифровая трансформация, риск-менеджмент, цифровизация, искусственный интеллект, неопределённость, кибератаки.

Кіріспе. Киберқауіпсіздік технологияның қарқынды дамуы мен кибершабуылдардың көбеюі жағдайында өте маңызды болады. Киберқауіпсіздік аудиті осалдықтар мен тәуекелдерді анықтау үшін ұйымның ақпараттық жүйелерін, процестері мен тәжірибелерін жүйелі түрде тексеру және бағалау болып табылады. Пандемия, экономикалық дағдарыстар және саяси тұрақсыздық сияқты жаһандық оқиғалардан туындаған белгісіздік жағдайында киберқауіпсіздік аудитінің өзектілігі айтарлықтай өсті. Бұл мақалада біз Қазақстандағы киберқауіпсіздіктің ағымдағы жай-күйін, соңғы үш жылдағы аналитикалық деректерді және белгісіздік жағдайында аудит жүргізудің маңыздылығын қарастырамыз (Осавелюк, 2023:33). Ғылыми мақаланың мақсаты белгісіздік факторларын ескере отырып, киберқауіпсіздік аудитін жүргізудің теориялық және практикалық аспектілерін кешенді зерттеу, сондай-ақ ақпараттық жүйелердің қорғалу деңгейін бағалаудың тиімділігін арттыру бойынша тәсілдер мен ұсыныстарды әзірлеу болып табылады. Зерттеу киберқауіпсіздік аудиті шеңберінде киберқауіпсіздіктер, оларды анықтау және бағалау әдістері, сондай-ақ бастапқы деректер мен сыртқы ортаның белгісіздік дәрежесі арасындағы байланысты анықтауға бағытталған.

Зерттеудің міндеттері киберқауіпсіздік аудитінің теориялық және әдіснамалық негіздерін талдау, толық емес ақпарат жағдайында киберқауіпсіздік аудитінің әдістері мен құралдарын зерттеу, қауіпсіздік деңгейін бағалауға әсер ететін белгісіздік факторларын анықтау, сондай-ақ толық емес және дәл емес ақпарат жағдайында аудиторлық процедуралардың тиімділігін арттыру бойынша ұсыныстар әзірлеу болып табылады.

Бұл мақала киберқауіпсіздік пен осалдық туралы ақпараттың толық емес, дәл емес және өзгергіштігі жағдайында ұйымдардың киберқауіпсіздік деңгейін және цифрлық активтерін бағалау процестерін, әдістері мен құралдарын зерттеуге арналған. Осы тақырып шеңберінде киберқауіпсіздік пен аудиттің теориялық негіздері қарастырылады, ақпараттық қауіпсіздік саласында шешімдер қабылдауға әсер ететін белгісіздік көздері мен түрлері талданады, сондай-ақ қолданыстағы аудит стандарттары мен әдістемелерінің қолданылуы бағаланады. Динамикалық өзгеретін кибер орта жағдайында оның сенімділігі мен тиімділігін арттыруға бағытталған аудит жүргізуге тәуекелге бағдарланған және бейімделгіш тәсілдерге ерекше назар аударылады.

Киберқауіпсіздік аудиті ұйымдардағы бақылау құралдарының болуы мен тиімділігін бағалауға бағытталған процесс. IT-инфрақұрылымдағы осалдықты анықтайды, халықаралық және ұлттық стандарттарға сәйкестігін бағалайды, тәуекелдерді басқару процестерін жақсартады, мүдделі тараптардың сенімін арттырады. Белгісіздік пен өсіп келе жатқан қауіп-қатер жағдайында киберқауіпсіздіктің тәуелсіз аудиті мемлекеттік қызметтер, қаржы секторы, телекоммуникация және маңызды инфрақұрылым үшін стратегиялық ресурсқа айналады, өйткені тексеру нәтижелері қорғаныс шараларын жедел түзетуге және ықтимал шығындарды азайтуға мүмкіндік береді(Аверченков, 2021:37-38).

Тиімді киберқауіпсіздіктің негізгі аспектілерінің бірі-көп деңгейлі қорғанысты енгізу. Бұған кіруді анықтау және алдын алу жүйелері (IDS/IPS), антивирустық бағдарламалар, брандмауэрлер және соңғы нүктелерді қорғау шешімдері сияқты әртүрлі технологияларды пайдалану кіреді. Дегенмен, технология - теңдеудің бір бөлігі ғана. Адам факторы да маңызды рөл атқарады: қызметкерлерге қауіпсіздік бойынша тұрақты жаттығулар сәтті шабуылдардың қаупін айтарлықтай төмендетуі мүмкін. Сонымен қатар, ұйымдар киберқауіптер туралы ақпаратты пайдалану және басқа компанияларда болған оқиғаларды талдау арқылы жаңа қауіптер мен осалдықтарды белсенді түрде бақылауы керек. Бұл ақпарат жақсырақ қорғаныс стратегияларын әзірлеуге және жалпы киберқауіпсіздікті жақсартуға көмектеседі. Деректердің сақтық көшірмесін жасаудың маңыздылығын да есте ұстаған жөн. Сақтық көшірмелерді үнемі жасау шабуылдаушылар деректерді шифрлап, төлемді талап еткен кезде бопсалау сияқты сәтті шабуыл кезінде зиянды азайтуға мүмкіндік береді. Ағымдағы резервтік көшірмелердің болуы бизнестің өмірлік тірегі бола алады, бұл оның жұмысын айтарлықтай шығынсыз қалпына келтіруге мүмкіндік береді. Қорытты айытқанда, киберқауіпсіздік — бұл технологияның жиынтығы ғана емес, сонымен қатар технологияны, процестерді және адамдарды қамтитын кешенді тәсіл. Ұйымның барлық деңгейлеріндегі үйлестірілген күш-жігер ғана үнемі дамып келе жатқан киберқауіптерден сенімді қорғауды қамтамасыз ете алады.

Киберқауіпсіздік аудитін жүргізудің әдістемелік тәсілдері бар, олар белгісіздікті арнайы ескереді-мысалы, ақпараттың жетіспеушілігі, тез өзгеретін қауіпті орта және шектеулі ресурстар. Киберқауіпсіздік аудитін жүргізудің негізгі әдістемелік тәсілдеріне мыналар жатады:

1. тәуекелге бағытталған тәсіл (Risk-Based Audit). Бұл белгісіздік жағдайында сценарийлік талдаулар мен сараптамалық бағалаулар қолданылатын бизнес-процестерде ықтимал қауіптер мен осалдықтарға ұшырайтын ақпараттық активтерді пайдаланатын ұйымдар үшін қолданылады;
2. бақылау (Compliance) тәсілі. Белгісіздікке бейімделуді ескере отырып, стандарттарға сәйкестікті тексеру (ISO/IEC 27001, NIST, GDPR және т. б.);
3. сценарий-аналитикалық тәсіл (Scenario-Based Audit). Оқиғалардың ықтимал сценарийлерін әзірлеу және олардың әсерін модельдеу. (SWOT-киберқауіпсіздік қауіптерін талдау, киберқауіпсіздіктерге реакцияны бағалау үшін Tabletop exercises, барлау деректерін пайдалана отырып қауіптерді болжау (Threat Intelligence);
4. итеративті және адаптивті аудит (Agile / Adaptive Audit). Аудит алынған нәтижелерге байланысты мақсаттар мен әдістерді үнемі түзете отырып, қайталанулар бойынша жүргізіледі.

Киберқауіпсіздік аудитін жүргізудің әдістемелік тәсілдері ақпараттық қауіпсіздікті тексеру процесін құрылымдауға көмектеседі. Бірақ аудиторлық процедураның өзі нақты

пайда әкелген жағдайда ғана мағынасы бар: тәуекелдерді азайтады, жүйелердің тұрақтылығын арттырады және ресурстарды пайдалануды оңтайландырады. Белгісіздік жағдайында аудиттің қаншалықты тиімді екенін және қандай критерийлер оны бағалауға мүмкіндік беретінін анықтау өте маңызды. Белгісіздік жағдайында киберқауіпсіздік аудитін бағалау критерийі оның толық емес, өзгермелі және ықтималды деректермен жұмыс істеу кезінде жүйенің тәуекелдері мен тұрақтылығы туралы негізделген және басқарушылық шешімдер қабылдауға жарамды қорытындыларды қамтамасыз ету қабілеті болып табылады. Бұл өлшемге қол жеткізу киберқауіпсіздік аудитін кезең-кезеңімен жүргізу арқылы қамтамасыз етіледі.

Бірінші кезең-аудиттің мақсаттары мен көлемін анықтау, онда тексерілетін жүйелер мен процестердің тізімі белгіленеді, сонымен қатар аудиттің негізгі міндеттері тұжырымдалады. Бұдан әрі нормативтік және техникалық құжаттаманы талдауды, қызметкерлермен сұхбат жүргізуді және ақпаратты қорғаудың қолданыстағы шараларын бағалауды қамтитын ақпарат жинау жүзеге асырылады. Жиналған мәліметтер негізінде тәуекелдерді бағалау кезеңі орындалады, оның шеңберінде осалдықтар анықталады және оларды ұйымның қызметі үшін іске асырудың ықтимал салдары талданады.

Келесі кезең-киберқауіпсіздік деңгейін арттыруға және анықталған тәуекелдерді азайтуға бағытталған ұсыныстарды әзірлеу. Соңғы кезең-ұсынылған шаралардың іске асырылуын бақылауды және өзгеріп отыратын қауіпті орта жағдайында олардың тиімділігін үнемі бағалауды көздейтін мониторинг және қайта аудит.

Тиімділікті бағалау-қолданылатын шараларды, олардың қауіптен қорғау стратегияларын іске асырудың практикалық тиімділігін талдау. Бұл кезең жоғары белгісіздік жағдайында жүйелердің тұрақтылығы үшін маңызды (Козырь, 2025:338).

Қазақстанда киберқауіпсіздік аудитін жүргізу бірқатар проблемаларға тап болады:

- жетілудің төмен деңгейі киберқауіпсіздік аудиті;
- киберқауіпсіздік саласындағы шетелдік шешімдерге тәуелділік;
- корпоративтік тәуекелдерді басқаруда киберқауіпсіздік аудитінің жеткіліксіз интеграциясы;
- Қазақстандағы киберқауіпсіздік мәселелерінде аккредиттелген аудиторлық ұйымдардың шектеулі саны.

ҚР Ұлттық Банкі 2022 жылы екінші деңгейдегі банктердің міндетті киберқауіпсіздік аудитін енгізді, бұл 2021 жылмен салыстырғанда табысты шабуылдар санын 12% - ға төмендетуге мүмкіндік берді. Мемлекеттік мекемелерде "Қазақстанның киберқалқаны" 2022-2025 бағдарламасы шеңберінде ақпараттық жүйелерге кешенді тексерулер жүргізіледі. Жасанды интеллект және цифрлық даму министрі Ж. Мәдиев еліміздің киберқауіпсіздігін қамтамасыз ету бойынша қабылданып жатқан шаралар туралы айтып берді. Цифрлық Кодекс шеңберінде жауапкершілікті күшейту, киберқауіпсіздік аудитін енгізу және басқа да шаралар арқылы дербес деректерді қорғау саласындағы заңнаманы өзектендіру жоспарлануда. Жергілікті ерекшеліктерге бейімделген ақпараттық қауіпсіздік аудитінің ұлттық стандартын әзірлеу. Киберқауіпсіздік саласындағы аудиторларды даярлау деңгейін арттыру, сертификаттау бағдарламасын құру. Қауіптерді болжамды талдау үшін аудит процестеріне жасанды интеллект пен big data енгізу. ШЫҰ және БҰҰ шеңберінде киберқорғау аудиті саласындағы тәжірибелермен алмасу бойынша халықаралық ынтымақтастықты кеңейту.

National Cyber Security Index Kazakhstan деректері бойынша қауіпсіздік индексі 48,05% болатын 176 елдің ішінде 78-ші орында. Дербес деректерді қорғау (100%) және кәсіптік білім беру (89%) саласында ең үлкен жетістіктерге қол жеткізілді, алайда цифрлық сервистерді қорғауда және әскери кибероперацияларда төмен көрсеткіштер байқалады. (Афанасьев, 2020:225-227).

Кибершабуылдар деректердің жоғалуын, қаржылық шығындарды және беделдің бұзылуын қоса алғанда, жойқын әсер етуі мүмкін. Сондықтан тұрақты аудиттің қажеттілігін елемеу компанияға оны жүргізу шығындарынан әлдеқайда қымбатқа түсуі мүмкін. Тәуекелдердің алдын алу және азайту қазіргі заманғы бизнес үшін негізгі міндеттерге айналады, бұл киберқауіпсіздік аудитін стратегиялық басқарудың маңызды элементіне

айналдырады. Киберқауіпсіздік аудиті бір реттік іс — шара емес, тұрақты процесс екенін ескеру маңызды. Ұйымдар аудитті тәуекелдерді басқарудың жалпы стратегиясына біріктіруі керек, сонымен қатар оны тұрақты негізде жүргізуі керек. Аудит жиілігі әртүрлі факторларға, соның ішінде бизнес көлеміне, салаға және бұрынғы қауіпсіздік оқиғаларына байланысты болуы мүмкін. Киберқауіпсіздік аудиті күрделі және ресурстарды қажет ететін процесс болып көрінгенімен, бұл компаниялардың ұзақ мерзімді өмірін айтарлықтай жеңілдетеді. Өз тәуекелдері туралы нақты түсінікпен ұйымдар қауіпсіздік бюджеттерін бөлу туралы негізделген шешімдер қабылдай алады және шынымен назар аударуды қажет ететін аспектілерге назар аудара алады. Киберқауіпсіздік аудитінің тағы бір маңызды құрамдас бөлігі-ұйым ішіндегі қауіпсіздік мәдениеті. Қызметкерлерді оқыту және олардың ықтимал қауіптер мен қорғаныс әдістері туралы хабардарлығын арттыру табысты киберқауіпсіздік стратегиясының ажырамас бөлігі болып табылады. Тұрақты тренингтер, семинарлар және инциденттерге дайындық тестілері адам факторына байланысты оқиғалардың қаупін айтарлықтай төмендетуі мүмкін (Баранова, 2019:154-155).

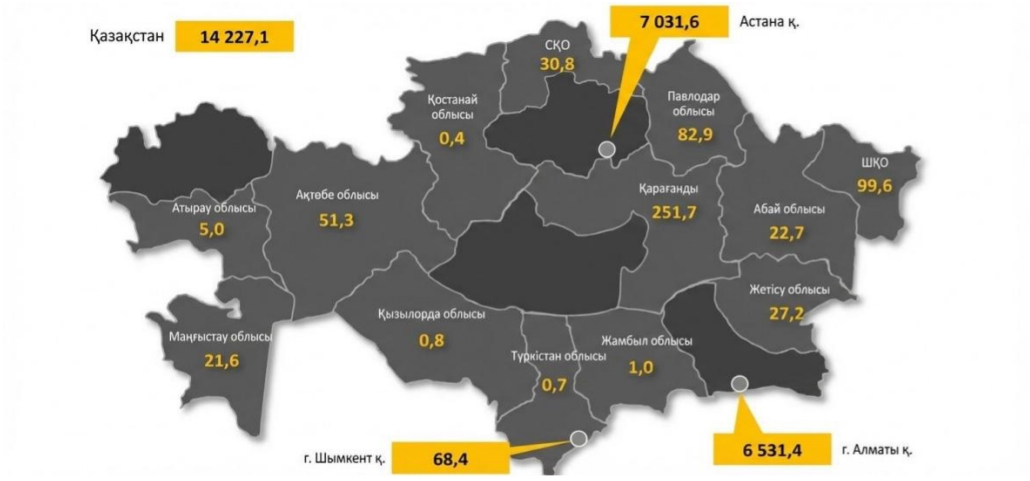
Осылайша, киберқауіпсіздік аудиті мен бағалауына қатысты бірнеше негізгі ойларды бөліп көрсетуге болады: осалдықтар мен тәуекелдерді анықтау үшін киберқауіпсіздік аудиті қажет; аудит әдістері ену тестілеуін, тәуекелдерді бағалауды және конфигурацияны талдауды қамтуы мүмкін; тұрақты аудиттер жүргізу қауіпсіздіктің жоғары деңгейін сақтауға көмектеседі; аудит нәтижелері бойынша ұсыныстарды жүзеге асыру тәуекелдерді азайту үшін маңызды; қауіпсіздік мәдениеті ұйымда оқиғалардың алдын алуда шешуші рөл атқарады.

Зерттеу материалдары мен әдістері. Цифрлық кеңістікке көбірек процестер тасымалданатын қазіргі әлемде киберқауіпсіздік кез келген компания үшін негізгі міндеттердің бірі болып табылады. Құпия ақпараттың ағып кетуі, кибершабуылдар және деректер қауіпсіздігінің бұзылуына байланысты басқа да оқиғалар бизнеске үлкен зиян келтіруі мүмкін. Сондықтан аудит жүргізу және киберқауіпсіздікті бағалау компанияның ақпараты мен өзге де цифрлық активтерін қорғауды қамтамасыз етудегі маңызды кезеңдер болып табылады.

Киберқауіпсіздік қазіргі әлемде өзекті тақырыпқа айналуда, мұнда цифрлық технологиялар біздің күнделікті өміріміз бен кәсіпкерімізде маңызды рөл атқарады. Кибершабуылдар мен құпия ақпараттың ағып кетуінің артуымен компаниялар өздерінің цифрлық ресурстарының қауіпсіздігін бағалау және қамтамасыз ету қажеттілігіне көбірек назар аударуда.

Киберқауіпсіздікті тексеру және бағалау-бұл компьютерлік жүйелердегі, желілердегі және қосымшалардағы ақпаратты қорғау деңгейін тексеру, бағалау және жақсарту процесі. Бұл процестер қауіпсіздіктің осалдықтары мен кемшіліктерін анықтауға, сондай-ақ оларды жою және қорғаудың жалпы деңгейін жақсарту бойынша ұсыныстар жасауға мүмкіндік береді.

Нәтижелер және талқылау. Цифрлық технологиялардың қарқынды дамуы және киберқауіптердің көбеюі жағдайында киберқауіпсіздік аудиті мен бағалауы өз деректерінің сақталуын және ақпараттық қауіпсіздікті бағалайтын кез келген ұйым жұмысының ажырамас бөлігіне айналады. Бұл процестер ықтимал тәуекелдерді анықтап қана қоймай, сонымен қатар қорғаныс деңгейін тиімді бақылауға және нақты уақыттағы қауіптерге тез жауап беруге мүмкіндік береді (ВасильеваКуприянов, 2023:207-212). Бұл процестер әлеуетті киберқауіптерді анықтап қана қоймай, ақпараттық жүйелердің қорғалу деңгейін тиімді бақылауға, сондай-ақ нақты уақыттағы қауіп-қатерлерге жедел ден қоюға мүмкіндік береді.



Сурет 1. Киберқауіпсіздік саласындағы кәсіпорындар мен жеке кәсіпкерлерге көрсетілген қызметтер көлемі (млн. теңге)

Аталған процестердің практикалық іске асырылуы Астана, Алматы, Қарағанды, Қостанай, Түркістан, Қызылорда, Ақмола, Алматы, Батыс Қазақстан және Ұлытау облыстарындағы киберқауіпсіздік саласындағы кәсіпорындар мен жеке кәсіпкерлерге көрсетілетін қызметтер көлемінде көрініс табады, бұл аталған өңірлердегі киберқауіпсіздік шараларына сұраныс пен жетілу деңгейіндегі айырмашылықтарды көрсетеді. 1-сурет көрсеткендей. киберқауіпсіздік саласындағы қызметтер көлемі 2023 жылғы қаңтар – қыркүйекте 14,2 млрд теңгеге жетті — бір жыл бұрынғыға қарағанда ақшамен бірден 2,6 есе көп. Өңірлік бөліністе киберқауіпсіздік саласында ең көп қызметтер Астанада көрсетілді: 7 млрд теңгеге — өткен жылмен салыстырғанда екі есе көп. Екінші және үшінші жолдарда Алматы (6,5 млрд теңге, жылдық өсім — бірден 4,9 есе) және Қарағанды облысы (251,7 млн теңге, плюс 39,9%) орналасқан. Мұндай қызметтердің ең азы Қостанай, Түркістан және Қызылорда облыстарында көрсетілді. Ақмола, Алматы, Батыс Қазақстан және Ұлытау облыстарында салада қызметтер тіркелген жоқ.

Кесте 1. Киберқауіпсіздік оқиғаларының санын талдау 2023-2024 ж.ж. *Ескерту: авторлар дереккөз негізінде құрастырған - https://stat.gov.kz/ru/*

№	Атауы	2023 ж.		2024 ж.	
		мың шабуыл	үлес салмағы, %	мың шабуыл	үлес салмағы, %
1	Компьютерлік вирустар, желілік құрттар, трояндар	1653	78,6	2795	66,7
2	Интернеттегі фишинг	41	2,0	594	14,2
3	Ботнет-шабуылдар	133	6,3	322	7,6
4	Интернет-ресурсқа қолжетімділіктің болмауы	86	4,0	88	2,1
5	Қызмет көрсетуден бас тарту (DoS / DDoS шабуылы)	20	4,6	16	0,3
6	Рұқсатсыз қол жеткізу және мазмұнды модификациясы	93	4,4	5	0,4
7	Басқа оқиғалар	77	0,1	366	8,7
	Барлығы	**2103**	**100**	**4186**	**100**

Осы кестеде көрсетілгендей, 2024 жылы Қазақстанда 2023 жылмен салыстырғанда 4186 мың кибершабуыл тіркелді — бұл өткен жылмен салыстырғанда бірден екі есе көп.

Кибершабуылдар құрылымындағы ең үлкен үлес компьютерлерді зиянды вирустармен, желілік құрттармен және трояндармен жұқтыру болды, жалпы жиынтықтың 66,7% немесе 2 795 мың жағдай. Интернет желісіндегі фишингтік шабуылдардың саны жалпы қорытындының 14,2% немесе 594 мың шабуылды құрады, бұл 2023 жылмен салыстырғанда олардың саны 553 мың жағдайға өсті. Кибершабуылдар құрылымындағы өзге де оқиғалар жалпы қорытындының 8,7% -. немесе 366 мың шабуылды құрады, бұл 2023 жылмен салыстырғанда олардың саны 289 мың жағдайға артты. Кибершабуылдар құрылымында келесі кезекте botnet-шабуылдар тұр, олардың үлес салмағы 2024 жылы 7,6% немесе 322 мың кибершабуылды құрайды, бұл 2023 жылмен салыстырғанда 189 мың жағдайға артып келеді. Интернет-ресурсқа қол жетімділіктің болмауы, рұқсатсыз қол жетімділік және мазмұнды өзгерту, қызмет көрсетуден бас тарту (DoS/ DDoS шабуылы) кибершабуылдар құрылымында соңғы орындарды алады. Сонымен қатар, DoS / DDoS шабуылдарының саны 20% — ға, 16 жағдайға дейін, ал рұқсатсыз қол жеткізу және мазмұнды модификация оқиғаларының саны бұрынғы жағдаймен салыстырғанда азайды.

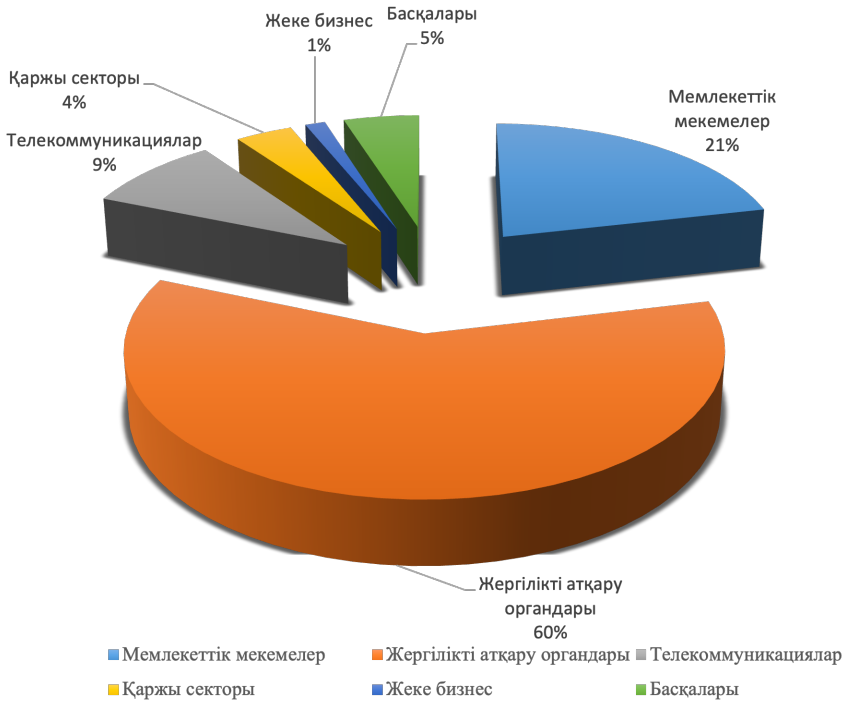


Диаграмма 1. 2024 жылғы кибершабуылдардың жалпы санының үлесі. *Ескерту: авторлар дереккөз негізінде құрастырған https://www.gov.kz/*

Соңғы жылдары Қазақстан үшін өзекті киберқауіптерді зерттеу барысында Қазақстанда киберқылмыстардың ең жиі құрбандары анықталды 2024 жыл телекоммуникациялар 9%, мемлекеттік органдар 23%, жеке бизнес 1%, қаржы секторы 4% және жергілікті атқарушы орган 63% болды. Жеке және тіркелгі деректері үлкен сұранысқа ие болды. Ұлттық компьютерлік инциденттерге әрекет ету қызметінің сарапшылары инфостилерлер деп атады, олардың көмегімен зиянкестер жеке деректерді ұрлап кетті. Сондай-ақ, компаниялардың серверлерінде үлкен көлемдегі деректер сақталатынын және өңделетінін атап өткен жөн. Телекомға жасалған әрбір төртінші шабуылдың нәтижесінде құпия ақпарат тарады. Зиянкестер провайдердің басып алынған инфрақұрылымын айлар, тіпті жылдар бойы бақылай алады, одан құнды мәліметтерді үнемі түсіріп отырады. Осыған қарамастан, аймақтың цифрлық трансформациясы қарқын алуда. Бұл сөзсіз киберқылмыскерлердің назарын аударады. Әр тоқсан сайын шабуылдар саны артып келеді, сондықтан мемлекеттік сектор мен бизнес субъектілері өздерінің қорғанысын күшейтуі керек.

Зерттеу мақсатында келесі әдістер қолданылды:

- аналитикалық әдіс-Қазақстан Республикасының киберқауіпсіздік саласындағы нормативтік-құқықтық базасын талдау;
- статистикалық әдіс-CERT-KZ, ЦДИАӨМ ақпараттандыру комитеті, ҚР Ұлттық Банкі және Global Cybersecurity Index деректерін өңдеу;
- салыстырмалы талдау әдісі-Қазақстанның көрсеткіштерін Орталық Азияның басқа елдерімен және ЕАЭО мүшелерімен салыстыру;
- сараптамалық бағалау әдісі-консалтингтік компаниялардың сұхбаттары мен салалық есептерінен қорытындыларды жинақтау (KPMG, Deloitte, PwC Kazakhstan);
- ұлттық және халықаралық рейтингтерге шолу — Ұлттық киберқауіпсіздік индексі мен аймақтық салыстырмалы зерттеулердің көрсеткіштерін қосу;
- киберқауіпсіздік аудитінің рөлі мен мазмұнын және оның әдіснамалық аспектілерін түсіну үшін нормативтік құжаттарды, зерттеулер мен сараптамалық жарияланымдарды контент-талдау;
- жаңа технологиялардың ықпалын, геосаяси жағдайдың тұрақсыздығын және қауіптердің эволюциясын қоса алғанда, IT және қауіптердің даму трендтерін сапалы талдау;
- осалдықтарды бағалау жүйелердегі әлсіз жерлерді іздеу;
- инциденттерге мониторинг және жауап беру — жауап берудің уақтылығы мен тиімділігін бағалау.

Киберқауіпсіздік аудитінің маңызды аспектісі бағалаудың әртүрлі әдістерін қолдану болып табылады:

- енуді тестілеу-осалдықтарды анықтау үшін жүйелерге шабуылдарды модельдеу;
- тәуекелдерді бағалау-бизнеске ықтимал қауіптер мен әсерлерді талдау;
- конфигурацияны талдау-жүйелер мен бағдарламалардың ең жақсы киберқауіпсіздік тәжірибесіне сәйкестігін тексеру;
- әлеуметтік инженерия-қызметкерлердің киберқауіптер туралы хабардарлық деңгейін тексеру.

Аудит нәтижелері, әдетте, анықталған осалдықтардың тізбесін, тәуекелдерді бағалауды және оларды жою жөніндегі ұсынымдарды қамтитын баяндама түрінде ұсынылады. Барлық мүдделі тараптар талқылауға және шешім қабылдауға қатыса алатындай ақпарат түсінікті тілде ұсынылуы керек. Киберқауіпсіздік аудитін жүргізудің себептері деректерді қорғау, нормативтік талаптарды сақтау, клиенттердің сенімін нығайту, киберқауіптерге төзімділік болып табылады.

2023-2025 жылдардағы оқиғалар динамикасын талдаудың салыстырмалы әдістері, сондай-ақ цифрлық жетілу деңгейі мен шабуыл жиілігі арасындағы корреляциялық талдау қолданылды.

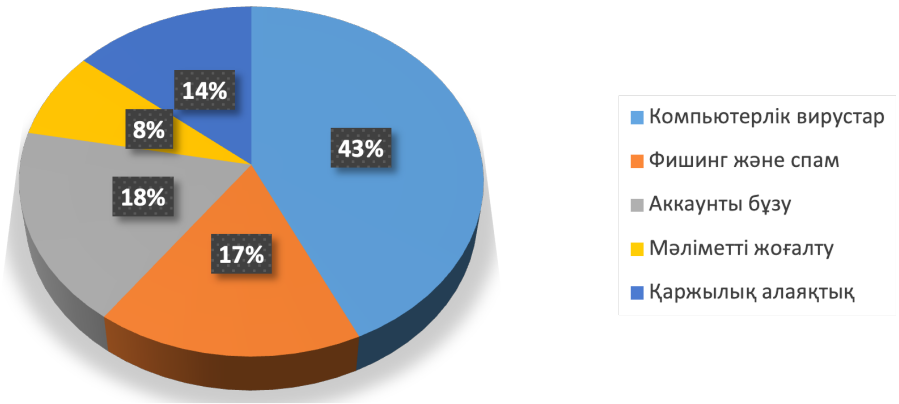


Диаграмма 2. Халық арасында киберқауіптер

Көрсеткіштерді талдау киберқауіптердің ең үлкен үлесін компьютерлік вирустар 42,8% құрайтынын көрсетеді, бұл соңғы құрылғылар мен зиянды бағдарламаларды тарату

арналарының жоғары осалдығын көрсетеді, сонымен қатар 18,1% есептік жазбаны бұзу және фишинг пен спам 16,9% маңызды тәуекелдер болып табылады. Бұл тіркелгі деректерін басқару және пайдаланушылардың әлеуметтік инженерияға төзімділігі мәселелерін көрсетеді, ал 13,9% қаржылық алаяқтық тікелей экономикалық шығындарға айтарлықтай қауіп төндіреді, ал деректердің жоғалуы жиіліктің төмендеуіне қарамастан 8,3% құрайды, салдары бойынша аса қауіпті болып қалады және басым қорғау шараларын талап етеді.

Киберқауіпсіздік аудиті ұйымдарға осалдықтарды анықтауға және оқиғаларға жауап беруге дайындық деңгейін бағалауға мүмкіндік береді. Белгісіздік жағдайында, күтпеген көздерден қауіптер туындауы мүмкін, аудит әсіресе маңызды болады (Максуров, 2023:78-79).

Киберқауіпсіздік аудиті бойынша ұсыныстар:

- ең маңызды активтерге, бизнес-процестерге және ықтимал сәтсіздік нүктелеріне назар аудара отырып, тәуекелге бағытталған тәсілді қолдану;
- сценарийлік талдау мен қауіп-қатерді модельдеуді, соның ішінде екіталай, бірақ жоғары импакты оқиғаларды қолдану;
- бағалаудың ресми әдістерін сараптамалық пайымдаулармен үйлестіре отырып, бастапқы деректердің толық еместігі мен өзгергіштігін ескеру;
- қауіпті жағдай өзгерген сайын қорытындылар мен ұсынымдарды тұрақты қайта қараумен аудитті итеративті түрде жүргізу;
- қорғаныс шараларының болуын ғана емес, сонымен қатар олардың бейімделуін, тұрақтылығын және тез қалпына келу қабілетін бағалау;
- болжанбайтын сценарийлер жағдайында инциденттерге жауап беру және басқару процестерінің дайындығын тексеру;
- шарттар өзгерген кезде түзетуге мүмкіндік беретін іске асырудың басымдықтары мен баламалы нұсқалары бар ұсынымдарды қалыптастыру.

Осылайша, белгісіздік жағдайында киберқауіпсіздік аудиті икемді, қайталанатын және тәуекелдерді басқаруға бағытталған болуы керек, бұл ұйымға осалдықтарды уақтылы анықтау, өзгеретін қауіптерге бейімделу және ақпарат толық болмаса да негізделген шешімдер қабылдау мүмкіндігін қамтамасыз етеді.

Қорытынды. Белгісіздік жағдайындағы киберқауіпсіздік аудиті Қазақстандағы ұйымдар үшін тәуекелдерді басқару стратегиясының ажырамас бөлігіне айналады. Кибершабуылдар санының өсуі мен қауіп-қатер ландшафтының өзгеруін ескере отырып, мемлекеттік сектор мен бизнес субъектілері тұрақты аудитті жүргізіп қана қоймай, сонымен қатар өздерінің киберқауіпсіздік стратегияларын жаңа жағдайларға бейімдеуі керек. Киберқауіпсіздікке инвестиция салу, қызметкерлерді оқыту және заманауи технологияларды енгізу тәуекелдерді айтарлықтай төмендетіп, ұйымдардың кибершабуылдарға төзімділігін арттыруы мүмкін. Дұрыс жүргізілген сауалнама мен бағалау компания тап болуы мүмкін осалдықтар мен тәуекелдерді анықтауға, сондай-ақ осалдықтарды жою және деректерді қорғау жүйесін жақсарту шараларын әзірлеуге мүмкіндік береді. Осылайша, тиімді киберқауіпсіздік аудиті бизнесті қорғап қана қоймайды, сонымен қатар оның белгісіздік жағдайында сәтті дамуына ықпал етеді.

Әдебиеттер

Аверченков, 2021 - Аверченков В.И. Аудит информационной безопасности. Учебное пособие. - М.: Флинта, 2021. - 679 с. ISBN: 978-5-9765-1256-6 [Rus]

Афанасьев, 2020 – Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. - 438 с. ISBN 978-5-99-12-0257-2 [Rus]

Баранова, 2019 - Баранова Е.К. Информационная безопасность и защита информации. Учебное пособие. - М.: Инфра-М, РИОР, 2019. – С.368 [Rus]

Бюро национальной статистики агентства по стратегическому планированию и реформам Республики Казахстан. [Электронный ресурс]. – Режим доступа: - https://stat.gov.kz/ru/ [Rus]

Васильева&Куприянов, 2023 - Васильева Т.Ю., Куприянов А.И. Информационная безопасность.- Учебн. М.: КноРус.-2023. – С.372. [Rus]

Козырь, 2025 - Козырь, Н.С. Аудит информационной безопасности: учебник для вузов. — Москва: Издательство Юрайт, 2025. — С.36. [Rus]

Комитет по правовой статистике и специальным учетам Генеральной прокуратуры РК [Электронный ресурс]. – Режим доступа: https://www.gov.kz/memleket/entities/pravstat [Rus]
Максуров, 2023 - Максуров А.А. Обеспечение информационной безопасности в сети Интернет. Монография. М.: Инфра-М.-2023.С.-226. ISBN 978-5-16-018251-3 [Rus]
Осавелюк, 2023 - Осавелюк Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ. Монография. М.: Лань. - 2023. -С.92. ISBN 978-5-507-47137-9[Rus]

References

Averchenkov, 2021 - Averchenkov V.I. Audit informacionnoj bezopasnosti [Information security audit]. Uchebnoe posobie. - M.: Flinta, 2021. - 679 c. ISBN: 978-5-9765-1256-6 [Rus]
Afanas`ev, 2020 – Afanas`ev A.A. Autentifikaciya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informacionny`m resursam [Authentication: Theory and Practice of Ensuring Secure Access to Information Resources]. Uchebnoe posobie dlya vuzov. - M.: Goryachaya liniya - Telekom, 2020. - 438 c. ISBN 978-5-99-12-0257-2 [Rus]
Baranova, 2019 - Baranova E.K. Informacionnaya bezopasnost` i zashhita informacii [Information security and information protection]. Uchebnoe posobie. - M.: Infra-M, RIOR, 2019. – S.368 [Rus]
Byuro nacional`noj statistiki agentstva po strategicheskomu planirovaniyu i reformam Respubliki Kazaxstan [Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan] [E`lektronny`j resurs]. – Rezhim dostupa: - https://stat.gov.kz/ru/ [Rus]
Komitet po pravovoj statistike i special`ny`m uchetam General`noj prokuratury` RK [E`lektronny`j resurs]. – Rezhim dostupa: https://www.gov.kz/memleket/entities/pravstat [Rus]
Kozy`r`, 2025 - Kozy`r`, N.S. Audit informacionnoj bezopasnosti: uchebnik dlya vuzov[Information Security Audit: A Textbook for Universities] - Moskva: Izdatel`stvo Yurajt, 2025. — S.36. [Rus]
Maksurov, 2023 - Maksurov A.A. Obespechenie informacionnoj bezopasnosti v seti Internet [Ensuring information security on the Internet]. Monografiya. M.: Infra-M.-2023.S.-226 ISBN 978-5-16-018251-3 [Rus]
Osavelyuk, 2023 - Osavelyuk E.A. Informacionnaya bezopasnost` gosudarstva i obshhestva v kontekste deyatel`nosti SMI [Information security of the state and society in the context of media activities]. Monografiya. M.: Lan`. - 2023. -S.92 [Rus]
Vasil`eva& Kupriyanov, 2023 - Vasil`eva T.Yu., Kupriyanov A.I., Informacionnaya bezopasnost`[Information security].- Uchebn. M.: KnoRus.-2023. – S.372. ISBN 978-5-507-47137-9[Rus]