ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

- Планируется ли проверка безопасности узлов сети?
- Будет ли внедрен мониторинг безопасности сети и решений?
- Каков план реагирования на инциденты, и кто за него отвечает?

Кроме того, Blockchain, так же как и другие формы распределенных реестров, может быть использован в качестве средства обеспечения информационной безопасности. В настоящее время наблюдается увеличение проектов в области кибербезопасности, основанных на этой технологии, таких как проверка целостности прошивок IoT-устройств, защита от DDoS-атак, децентрализованная идентификация и аутентификация, новое поколение инфраструктуры открытых ключей и др.

Список использованных источников

1. Frankfurt School Blockchain Center: Security in Blockchain Applications, 2018. https://fsblockchain.medium.com/security-in-blockchain-applications-43e73193512d

2. Md Rafiqul Islam, Md Mahmud, Ataur Rahman: A Review on Blockchain Security Issues and Challenges, 2021. https://www.researchgate.net/publication/354039550_A_Review_on_Blockchain_Security_Issues_and_Challenges

3. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen: A Survey on the Security of Blockchain Systems, 2020. https://csxqli.github.io/files/FGCS'20.pdf

4. A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE Percom workshop on security privacy and trust in the internet of thing, 2017

5. Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, in: International Journal of Web and Grid Services, 2016

6. Zamani E., He Y., Phillips M.: On the security risks of the blockchain. 2018. https://eprints.whiterose.ac.uk/143412/1/JCIS%20new%20manuscript%20FINAL%20NEW%20without%20codes.pdf

УДК 004.056.5

ӘЛЕМДІК КОМПАНИЯЛАРДЫҢ ҚАУІПСІЗДІК САЯСАТЫН ӘЗІРЛЕУ ТӘСІЛДЕРІ

Сарсембаев Нурбол Жалгасович
nur_bol_@mail.ru
магистрант, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.
Сагиндыков Каким Молдабекович
жетекші,т.ғ.к, доцент, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.

Аңдатпа. IBM, Sun Microsystems, Cisco Systems, Microsoft, Symantec, SANS және т.б. жетекші технологиялық компаниялардың тәжірибесіне негізделген ақпараттық қауіпсіздік саясатын құрудағы ең жақсы тәжірибелерге шолу жасайды. Өнеркәсіпте кеңінен танылған саясаттарды, процедураларды, стандарттарды және қауіпсіздік нұсқаулықтарын әзірлеу әдістері қарастырылуда. Ірі көшбасшы компаниялардың қауіпсіздік стандарттарын қалыптастыруға қатысуының маңыздылығы және олардың ақпаратты қорғаудың инновациялық тәсілдерін әзірлеудегі рөлі атап өтіледі. Бұл шолу ақпараттық қауіпсіздік тәжірибесін жақсартуға ұмтылатын ұйымдар үшін пайдалы нұсқаулық бола алады.

Кілт сөздер: қауіпсіздік саясаттары, процедуралар, қауіпсіздік стандарттары, технологиялық көшбасшы.

IBM компаниясының қауіпсіздік саясатын әзірлеуге көзқарасы: практикалық ұсыныстар

Ақпараттық қауіпсіздік саласындағы әлемдегі жетекші сарапшылардың бірі болып саналатын IBM көп жылдық тәжірибе мен озық стандарттарға негізделген қауіпсіздік

саясатын құрудың тиімді тәсілдерін ұсынады. IBM мамандарының ұсыныстарына сәйкес, корпоративтік қауіпсіздік құжаттарын әзірлеу ақпараттық қауіпсіздік саясатын қалыптастырудан басталуы керек. Бұл процесті компания ақпараттық тәуекелдерді басқарудың ажырамас бөлігі ретінде қарастырады.

IBM компаниясы белгілеген қауіпсіздік саясатын әзірлеудің негізгі кезеңдері келесі қадамдарды қамтиды:

Ақпараттық тәуекелдерді анықтау: мамандар компанияға барынша зиян келтіруі мүмкін тәуекелдерді талдаудан бастауды ұсынады, бұл олардың алдын алу үшін тиісті процедуралар мен шараларды әзірлеуге мүмкіндік береді.

Қауіпсіздік саясатын әзірлеу: қауіпсіздік саясаты Бизнестің мақсаттары мен міндеттеріне сәйкес келетін ақпараттық активтерді қорғау шараларын сипаттауы керек.

Төтенше жағдайлар жоспарларын қабылдау: қолданылатын шаралар оқиғалардың алдын алуға мүмкіндік бермейтін қауіпсіздік бұзылған жағдайда зиянды азайту үшін іс-қимыл жоспарларын әзірлеу қажет.

Қалдық ақпараттық тәуекелдерді бағалау: соңғы кезеңде қалдық тәуекелдерді бағалау және қаражат пен қауіпсіздік шараларына қосымша инвестициялардың қажеттілігі туралы шешім қабылдау жүргізіледі.

IBM ұсынған корпоративтік ақпараттық қауіпсіздік құжаттарының құрылымы мыналарды қамтиды:

Ақпараттық қауіпсіздікті және оны қамтамасыз ету бойынша Компания басшылығының ұстанымын айқындау.

Қауіпсіздік талаптарының сипаттамасы, соның ішінде заңнамаға сәйкестік, қызметкерлерді оқыту, вирустық шабуылдардың алдын алу және бизнестің үздіксіздігін жоспарлау.

Қызметкерлердің қауіпсіздікті қамтамасыз етудегі рөлдері мен міндеттерін және оқиғалар туралы есеп беру процесін сипаттау.

Корпоративтік қауіпсіздік саясаты құрылғаннан кейін саясатты іс жүзінде қолдану тәртібін анықтайтын стандарттар әзірленеді. Олар үнемі жаңартылып, ақпараттық қауіпсіздік саласындағы өзгеріп отыратын жағдайлар мен қауіптерге бейімделуі керек. Компания ұсынатын тәжірибелер мен рәсімдер қауіпсіздік ережелері мен нормаларын қалыптастыруға, тәуекелдерді талдауға және қорғау тәсілдерін ресімдеуге бағытталған, осылайша компанияның ақпараттық ресурстарының қауіпсіздігін тиімді басқаруды қамтамасыз етеді.

Қауіпсіздік саясатын дамыту: Sun Microsystems Компаниясының тәсілі

Ақпараттық технологиялар саласындағы танымал көшбасшы Sun Microsystems өзінің көп жылдық тәжірибесі мен озық стандарттарына негізделген қауіпсіздік саясатын әзірлеудің тиімді әдістерін ұсынады.

Қауіпсіздік саясаты, Sun Microsystems мәліметтері бойынша, ақпараттық қауіпсіздікті қамтамасыз етуге қатысты Компания басшылығының талаптарын білдіретін стратегиялық құжат. Маңыздысы, компания ақпаратты қорғау жүйесінің архитектурасын құруды бастамас бұрын қауіпсіздік саясатын әзірлеуден бастап жоғарыдан төменге қарай тәсілін қолдануды ұсынады.

Қауіпсіздік саясатын құруда рөлдер мен міндеттерді анықтау шешуші рөл атқарады. Sun Microsystems қауіпсіздік саясатын әзірлеу мен жүзеге асырудың кешенді тәсілін қамтамасыз ету үшін бизнесті басқару, техникалық басқару, ақпаратты қорғау бөлімі және басқалары сияқты компанияның әртүрлі бөлімшелерінің өкілдерін тартуға кеңес береді.

Ұсынылған қауіпсіздік саясаты құжаттарының құрылымы мыналарды қамтиды:

Ақпаратты қорғаудың мақсаттары мен міндеттерін сипаттау.

Басшылықтың қауіпсіздік саясатына қатынасын анықтау.

Саясатты іске асыру әдістерінің негіздемесі.

Қауіпсіздікке жауапты адамдардың рөлдері мен міндеттерін анықтау.

Қауіпсіздік ережелері мен нормаларын белгілеу.

Саясатты бұзғаны үшін жауапкершілікті анықтау.

Қауіпсіздік саясатын үнемі қайта қарау және бақылау.

Қауіпсіздік саясатының негізгі мақсаты-қызметкерлерді және компания басшылығын ақпараттық активтердің қауіпсіздігін қамтамасыз етудің талаптары мен тетіктері туралы хабардар ету. Саясат сонымен қатар стандарттарды, процедураларды және қауіпсіздік нұсқаулықтарын әзірлеуге негіз болады.

Sun Microsystems нұсқауларын орындай отырып, компаниялар ақпараттың сенімді қорғалуын қамтамасыз ететін және ақпараттық қауіптер қаупін азайтатын тиімді қауіпсіздік саясатын сәтті әзірлеп, енгізе алады.

Cisco Systems компаниясының тәсілі

Cisco мамандарының көзқарасы бойынша, желілік қауіпсіздік саясатының болмауы қауіпсіздік саласындағы елеулі оқиғаларға әкелуі мүмкін. Компанияның қауіпсіздік саясатын әзірлеуді желінің тәуекелдерін бағалаудан және оқиғаларға жауап беру бойынша жұмыс тобын құрудан бастау ұсынылады.

Cisco компаниясы құпия ақпаратты дұрыс қорғау үшін компания қызметкерлерінің рөлдері мен міндеттерін сипаттайтын пайдалану саясатын құруды ұсынады. Бұл ретте компанияның ақпараттық қауіпсіздік режимін ұйымдастырудың жалпы мақсаттары мен міндеттерін нақты белгілейтін негізгі қауіпсіздік саясатын әзірлеуден бастауға болады.

Келесі қадам-серіктестерге қандай ақпарат бар екендігі туралы хабарлау үшін серіктестерге рұқсат етілген пайдалану саясатын құру. Дұшпандық ретінде қабылданатын кез-келген іс-әрекетті, сондай-ақ мұндай әрекеттер анықталған кезде әрекет етудің мүмкін жолдарын нақты сипаттау керек.

Қорытындылай келе, қызметкерлердің есептік жазбаларын басқару және артықшылықтарды тексеру процедураларын сипаттау үшін әкімшілер үшін рұқсат етілген пайдалану саясатын құру қажет. Сонымен қатар, егер компанияда парольдерді қолдануға немесе ақпаратты санаттауға қатысты белгілі бір саясат болса, онда оны осында атап өту керек. Әрі қарай, аталған саясаттардың дәйектілігі мен толықтығын тексеру керек, сонымен қатар әкімшілерге қойылатын талаптардың оқу жоспарларында көрсетілгендігіне көз жеткізу керек.

Ақпараттық қауіпсіздік саясатын әзірлеу және іске асыру принциптері: Symantec компаниясының тәжірибесі

Ақпарат бизнестің негізгі активіне айналатын әлемде оның қауіпсіздігін қамтамасыз ету кез-келген компанияның Стратегиясының ажырамас бөлігіне айналды. Бұл тұрғыда Symantec тәуекелдерді, жауапкершілікті және қауіпсіздік стандарттарын анықтау сияқты негізгі аспектілерге назар аудара отырып, ақпараттық қауіпсіздік саясатын әзірлеу мен жүзеге асырудың негізгі кезеңдерін анықтайды.

Ақпараттық қауіпсіздік саясаты компанияның ақпараттық қауіпсіздік саласындағы мақсаттары мен міндеттерін анықтайтын маңызды стратегиялық құжат болып табылады. Symantec оны әзірлеу кезінде белгілі бір қадамдарды, соның ішінде активтерді анықтауды, тәуекелдерді бағалауды және қауіпсіздікті қамтамасыз етудегі келесі қадамдар үшін негіз болатын кешенді құжатты жасауды ұсынады.

Ақпараттық қауіпсіздік саясатының негізгі аспектілері қолдану саласы, қатаң сақтау қажеттілігі, саясат талаптарын бұзғаны үшін жауапкершілік пен салдарды анықтау болып табылады. Бұл саясаттың қауіпсіздік пен өнімділік арасында қарапайым, іске асырылатын және теңдестірілген болуы, сондай-ақ заң талаптарына сай болуы маңызды.

Қауіпсіздік саясатын тиімді іске асыру үшін саясаттың талаптары қалай орындалатынын және бақыланатынын дәл анықтайтын тиісті стандарттар мен рәсімдерді әзірлеу қажет. Бұл ISO 17799 талаптарына сәйкес келетін стандарттарды әзірлеуді, сондай-ақ қызметкерлердің күнделікті қызметінде басшылық болатын процедураларды белгілеуді қамтиды.

Тұтастай алғанда, ақпараттық қауіпсіздік саясатын әзірлеу және іске асыру - бұл егжей-тегжейге, ашықтыққа және жүйелік тәсілге назар аударуды қажет ететін кешенді процесс. Осы мақалада келтірілген Symantec тәжірибесінің арқасында компаниялар өздерінің Ақпараттық активтерін тиімді қорғайтын қауіпсіздік саясатын сәтті құрып, қолдай алады.

Пайдаланылған әдебиеттер тізімі

1. А.С. Петренко мен В.А.Курбатовтың «Политики безопасности компании при работе в Интернет» 2012. с.57-100
2. Петренко С.А., Симонов С. Экономически оправданная безопасность – журнал "IT Manager" № 15(3), 2008.
3. "The Design and Implementation of the FreeBSD Operating System" by Marshall Kirk McKusick, George V. Neville-Neil, Robert N.M. Watson 2014 с.
4. "Building Internet Firewalls" by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman 2000 с.88

УДК 336

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ НАЛОГОВОГО КОНТРОЛЯ И НАЛОГОВОГО КОМПЛАЕНСА

Сафонов Феликс Вячеславович
vsaffelix@gmail.com
магистрант 2 курса высшей школы финансов РЭУ им. Г.В. Плеханова
научный руководитель - Коваленко Светлана Николаевна

Аннотация. На сегодняшний день, налоговый контроль и комплаенс играют важную роль в управлении компанией – они позволяют предотвращать возможные риски и формировать налоговую политику компании. Вместе с этим современная практика налогового контроля и комплаенса сталкивается с вызовами в лице большего объема данных и задач. Решить данную проблему призваны специализированные информационные системы для налогов. Актуальность данной темы заключается в том, что за последние годы ИТ-системы стремительно развиваются, что в перспективы позволяет использовать их в решении проблем налогового контроля и комплаенса.

Ключевые слова: информационные системы, налоговый контроль, налоговый комплаенс, ИТ-архитектура, налогоплательщик, электронный документооборот, корпоративная отчетность, политики компании, расчетные показатели.

Под налоговым контролем понимается деятельность уполномоченных органов, направленная на обеспечение исполнения налогоплательщиками обязанностей по уплате налогов. К целям проведения налогового контроля относятся выявление нарушений, возникающих в рамках налогового законодательства; принятие шагов по их пресечению; а также сбор и анализ данных по уплате налогов для обеспечения достоверности соответствующей информации. Методы налогового контроля могут включать в себя следующие:

- Выборочную проверку некоторых документов;
- Проведение системного и логического анализа полученных данных;
- Применение инструментов статистики и экономического анализа;
- Группировку и кластеризацию документов в соответствие с их содержанием, и др.

Проведение налогового контроля объясняется необходимостью обеспечить регулярное получение налогов государством для пополнения своего бюджета. Как следствие, государству это нужно, чтобы оптимально выполнять свои функции по защите законных интересов налогоплательщиков. Налоги также позволяют стимулировать экономическую деятельность субъектов в государстве (например, за счет налоговых вычетов для граждан, предоставления налоговых каникул фирмам, повышения акцизов на импортируемые товары и т. д.). Таким образом, налоговый контроль играет важную в функционировании общественных институтов и проведении экономической политики в государстве в целом.

Вместе с этим современный налоговый контроль сталкивается с вызовами, существование которых объясняется такими причинами, как: увеличение объема