Цифрлық әдіскер
ақпараттық-білім беру ортасы

ДӘРІСТЕР ЖИНАҒЫ

Ақпараттық қауіпсіздік және ақпаратты қорғау

Ақпараттық қауіпсіздіктің негізгі принциптері — құпиялылық, тұтастық, қолжетімділік — және халықаралық стандарттар (ISO/IEC 27001, GDPR).

Құпиялылық, тұтастық, қолжетімділік
Аутентификация және авторизация
ISO/IEC 27001, GDPR
Қауіп-қатерлер

ДӘРІС ЖИНАҒЫ

ДӘРІС №1

Тақырыбы: Ақпараттық қауіпсіздік негіздері. Ақпараттық қауіпсіздіктің анықтамасы, мақсаты, принциптері, негізгі ұғымдары және стандарттары. Ақпараттық қауіпсіздік негіздері

Ақпараттық қауіпсіздіктің анықтамасы Ақпараттық қауіпсіздік — бұл ақпараттық ресурстарды (деректер, ақпараттық жүйелер, желілер, құрылғылар) рұқсатсыз қол жеткізуден, пайдаланудан, ашылудан, бұзылудан, өзгертілуден немесе жойылудан қорғауды қамтамасыз ету процесі. Ақпараттық қауіпсіздік барлық ақпаратты қорғауды, оның ішінде деректердің тұтастығын, қолжетімділігін және құпиялылығын қамтамасыз етуді қамтиды. Ақпараттық қауіпсіздік жеке тұлғалардың, ұйымдардың және мемлекеттің ақпараттық жүйелерінің қауіпсіздігін қамтамасыз етуге бағытталған. Бұл салада ақпаратты қорғау шаралары заңды, техникалық, ұйымдастырушылық, физикалық және басқарушылық әдістерді қамтиды. Ақпараттық қауіпсіздіктің мақсаты Ақпараттық қауіпсіздіктің негізгі мақсаты — ақпаратты қорғау арқылы ұйымның немесе тұлғаның қауіпсіздігін қамтамасыз ету. Ақпараттық қауіпсіздікті қамтамасыз ету үшін келесі негізгі мақсаттар қойылады: Ақпараттың құпиялылығын сақтау — ақпаратты рұқсатсыз тұлғалардан қорғау. Ақпараттың тұтастығын сақтау — ақпараттың толықтығын және дәлдігін сақтау, оны заңсыз өзгерістерден қорғау. Ақпараттың қолжетімділігін қамтамасыз ету — ақпаратқа рұқсат алған тұлғалардың оны уақтылы және толық қолжетімді ету. Ақпараттық қауіпсіздік шаралары осы үш маңызды мақсатты орындауға бағытталған. Ақпараттық қауіпсіздіктің принциптері Ақпараттық қауіпсіздіктің негізгі принциптері төменде көрсетілген: Құпиялылық (Confidentiality): Ақпараттың тек рұқсат алған тұлғаларға ғана қолжетімді болуын қамтамасыз ету. Құпиялылықты сақтау үшін шифрлау, аутентификация, кіру құқықтарын басқару сияқты әдістер қолданылады. Тұтастық (Integrity): Ақпараттың өзгертілмеуі немесе бұрмаланбауы керек. Яғни, ақпараттың бастапқы күйінде сақталуын қамтамасыз ету. Бұл үшін бақылау хештері мен деректердің тұтастығын тексеру әдістері қолданылады. Қолжетімділік (Availability): Ақпарат қажетті уақытта және қажетті жерде қолжетімді болуы керек. Қолжетімділікті сақтау үшін резервтік көшірмелер, серверлердің жұмысын қадағалау, апаттық қалпына келтіру шаралары пайдаланылады. Аутентификация (Authentication): Ақпарат жүйесіне қол жеткізу үшін пайдаланушының жеке басын дәл анықтау. Бұл пайдаланушының жүйеге кіруіне рұқсат беру үшін қажет. Авторизация (Authorization): Пайдаланушының белгілі бір ақпарат ресурстарына немесе жүйелік әрекеттерге рұқсат алған құқықтарын анықтау. Аудит (Audit): Жүйеде орындалған әрекеттерді бақылау, тіркеу және талдау. Бұл ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін қажет. Ақпараттық қауіпсіздіктің негізгі ұғымдары Ақпараттық жүйе: Ақпаратты жинау, өңдеу, сақтау және тарату үшін пайдаланылатын техникалық құралдар мен бағдарламалық қамтамасыз етудің жиынтығы. Қауіп-қатер: Ақпаратқа немесе ақпараттық жүйеге зиян келтіруі мүмкін фактор. Қауіпсіздік саясаты: Ақпараттық қауіпсіздікті қамтамасыз ету үшін ұйымның қабылдаған ережелері мен принциптері. Шабуыл: Ақпараттық жүйеге зиян келтіру мақсатында жасалған әрекет. Құпиялылықты бұзу: Ақпараттың рұқсатсыз немесе белгіленген құпиялылық деңгейінен асып кетуі. Ақпараттық инцидент: Ақпараттық жүйеде орын алған қауіпсіздік бұзушылығы немесе ақау. Ақпараттық қауіпсіздік стандарттары Ақпараттық қауіпсіздікті қамтамасыз ету үшін әртүрлі стандарттар мен нормативтік құжаттар қабылданған. Әлемдік және ұлттық деңгейде осы стандарттар бойынша қауіпсіздік шаралары мен талаптары анықталған. Осы стандарттардың кейбірі: ISO/IEC 27001 — ақпараттық қауіпсіздікті басқарудың халықаралық стандарты. ISO/IEC 27002 — ақпараттық қауіпсіздік шараларын жүзеге асыруға арналған нұсқаулық. NIST (National Institute of Standards and Technology) — АҚШ-тағы ұлттық қауіпсіздік стандарттарын және нұсқаулықтарын әзірлеуші ұйым. GDPR (General Data Protection Regulation) — Еуропалық Одақтың деректерді қорғау жөніндегі жалпы регламенті, жеке деректерді қорғауды қамтамасыз етеді. Бұл стандарттар ұйымдардың ақпараттық қауіпсіздік саясатын қалыптастыру және ақпараттық жүйелерді қорғау үшін маңызды негіздер ұсынады.

Бақылау сұрақтары: 1.Ақпараттық қауіпсіздіктің негізгі мақсаттары мен принциптерін атаңыз. 2.Ақпараттық қауіпсіздіктің құпиялылық, тұтастық және қолжетімділік принциптері қандай? 3.Ақпараттық жүйелердегі қауіптер мен шабуылдардың негізгі түрлерін сипаттаңыз. 4.ISO/IEC 27001 стандартының ақпараттық қауіпсіздікті басқарудағы рөлі қандай? 5.Ақпараттық қауіпсіздікті қамтамасыз ету үшін аутентификация мен авторизацияның маңызы қандай?

ДӘРІС №2

Тақырыбы: Ақпараттық жүйелердің классификациясы. Ақпараттық жүйелердің түрлері, олардың құрылымы мен қызметі. Әр түрлі қауіпсіздік деңгейлері мен қауіп-қатерлерді анықтау.

Ақпараттық жүйелердің классификациясы Ақпараттық жүйе — бұл деректерді жинау, өңдеу, сақтау, іздеу және тарату үшін қолданылатын техникалық, бағдарламалық және ұйымдық құралдардың жиынтығы. Ақпараттық жүйелер белгілі бір мақсаттарды іске асыру үшін ақпаратты тиімді басқаруға арналған. Ақпараттық жүйелер бірнеше белгілері бойынша классификацияланады: Қызметі мен қолдану саласына қарай: Шаруашылық жүйелері: өндіріс, экономика, қаржы саласында жұмыс істейді. Мысалы, кәсіпорындардың бухгалтерлік есеп жүйелері. Ғылыми және инженерлік жүйелер: ғылыми зерттеулер, инжинирингтік есептеулер және жобалау жұмыстары үшін қолданылады. Әкімшілік жүйелер: мемлекет және жергілікті билік органдарында әкімшілік шешімдер қабылдауға арналған жүйелер. Медициналық жүйелер: медициналық ақпаратты жинау және өңдеу үшін, аурухана мәліметтерін басқаруға арналған жүйелер. Әлеуметтік жүйелер: білім беру, заң, мәдениет саласындағы ақпаратты басқару жүйелері. Қолдану деңгейіне қарай: Стратегиялық деңгейдегі жүйелер: ұйымның ұзақ мерзімді стратегияларын басқаруға арналған жүйелер. Тактикалық деңгейдегі жүйелер: ұйымның орта мерзімді міндеттерін шешу үшін арналған жүйелер. Оперативтік деңгейдегі жүйелер: күнделікті операциялық жұмысқа арналған жүйелер. Құрылымдық компоненттеріне қарай: Автономды жүйелер: тек бір ғана құрылғыдан тұратын және өздігінен жұмыс істейтін ақпараттық жүйелер. Тарату жүйелері: бірнеше құрылғылардан немесе компоненттерден тұратын, желі арқылы байланысатын жүйелер. Ақпараттық жүйелердің түрлері, құрылымы мен қызметі Ақпараттық жүйелердің түрлері олардың қызметіне, құрылымына және қолдану саласына қарай әртүрлі болады. Олардың негізгі түрлерін қарастырайық: Операциялық жүйелер (Operational Systems): Бұл жүйелер ұйымның күнделікті жұмысын қолдайды, мысалы, сату немесе өндіріс бойынша мәліметтерді өңдеу, есеп жүргізу. Құрылымы: мәліметтер базасы, қосымшалар, пайдаланушылар интерфейсі. Қызметі: ақпарат жинау, сақтау, өңдеу, пайдаланушыға ұсыныс жасау. Аналитикалық жүйелер (Analytical Systems): Қаржылық немесе статистикалық талдауды жүргізу үшін қолданылады. Мысалы, бизнес талдау жүйелері. Құрылымы: деректер қоймасы (Data Warehouse), аналитикалық құралдар. Қызметі: үлкен деректерді талдау, есептер мен шешімдер ұсыну. Қаржылық басқару жүйелері (Financial Management Systems): Қаржы есептерін жүргізу және ақша ағындарын басқару үшін қолданылады. Құрылымы: бухгалтерлік есеп деректер базасы, қаржы жоспарлау құралдары. Қызметі: төлемдер мен кірістерді бақылау, бюджетті жоспарлау, қаржылық есеп беру. Қызмет көрсету жүйелері (Customer Service Systems): Пайдаланушылардың сұраныстарын қанағаттандыру және олармен өзара әрекеттесу үшін қолданылады. Құрылымы: клиент деректер базасы, қызмет көрсету қосымшалары. Қызметі: клиенттермен байланыс орнату, қызмет көрсету сапасын бақылау. Қоғамдық жүйелер (Public Systems): Мысалы, мемлекеттік органдар немесе университеттердің ақпараттық жүйелері. Құрылымы: мәліметтер базасы, ақпарат жинау құралдары. Қызметі: азаматтарға немесе студенттерге қызмет көрсету, мемлекеттік деректерді жинау және тарату. Интернет-қосымшалар және веб-жүйелер (Web-based Systems): Бұл жүйелер интернет немесе интра—жүйелер арқылы жұмыс істейді. Мысалы, электрондық коммерция, онлайн банкинг жүйелері. Құрылымы: веб-сервер, қолданушы интерфейсі, мәліметтер базасы. Қызметі: клиентпен байланыс, интернет арқылы қызмет көрсету. Қауіпсіздік деңгейлері мен қауіп-қатерлерді анықтау Ақпараттық қауіпсіздік деңгейлері мен қауіп-қатерлерді анықтау, ақпараттық жүйелерді қорғау үшін маңызды әдіс болып табылады. Әрбір жүйе үшін арнайы қауіпсіздік деңгейлері мен мүмкін қауіптер анықталады. Қауіпсіздік деңгейлері: Төмен деңгей (Low): Ақпараттың құпиялылығына, тұтастығына және қолжетімділігіне байланысты тәуекелдер төмен. Бұл деңгейде қолданушылардың сұрау бойынша ақпаратты өңдеу немесе тарату әрекеттері аз болады. Орта деңгей (Medium): Ақпараттың құпиялылығы мен тұтастығын сақтаудың маңызы жоғары. Бұл деңгейде қауіпсіздік шаралары орташа күшті болады. Жоғары деңгей (High): Бұл деңгейдегі ақпарат өте құпия және жоғары деңгейдегі қауіпсіздік шараларын талап етеді. Құпия деректерді қорғау үшін шифрлау, аутентификация, аудит және басқа да құралдар пайдаланылады. Қауіп-қатерлерді анықтау: Қауіп-қатерлерді анықтау кезінде төмендегідей факторлар ескеріледі: Шабуылдар: зиянды бағдарламалар, хакерлік шабуылдар, фишинг, вирус жұқтыру. Желілік қауіптер: деректерді ұрлау, жүйеге рұқсатсыз кіру, желілік шабуылдар. Құпиялылық бұзылуы: пайдаланушының жеке деректерінің жариялануы немесе рұқсатсыз қолжетімділігі. Деректердің тұтастығының бұзылуы: деректердің өзгертілуі, бүлінуі немесе жоғалуы. Қолжетімділіктің төмендеуі: жүйенің немесе мәліметтердің уақытша қолжетімсіз болуы. Қауіп-қатерлерді анықтаудың негізгі кезеңдері: Қауіп-қатерлерді талдау: Жүйелердегі ықтимал қауіп-қатерлер мен олардың ықтимал әсерін бағалау. Тәуекелді басқару: Қауіптерді анықтау, бағалау және соларға қарсы шараларды қабылдау. Қауіпсіздік шараларын қолдану: Қауіп-қатерлерді азайту мақсатында алдын алу шараларын қолдану.

Бақылау сұрақтары: 1.Ақпараттық жүйелерді қандай белгілер бойынша классификациялауға болады? 2.Ақпараттық жүйелердің құрылымын сипаттаңыз және олардың қызметтерін түсіндіріңіз. 3.Қауіпсіздік деңгейлері қандай және олар қандай факторларға байланысты анықталады? 4.Ақпараттық жүйелердің қауіптерін анықтау әдістері қандай? 5.Ақпараттық жүйелерде қандай негізгі қауіп-қатерлер кездеседі және олардан қорғау жолдары қандай?

ДӘРІС №3

Тақырыбы: Ақпаратты қорғаудың заңды және нормативтік негіздері. Ақпараттық қауіпсіздікті қорғауға қатысты халықаралық және ұлттық заңдар, стандарттар және ережелер.

Ақпараттық қауіпсіздікті қорғаудың заңды және нормативтік негіздері Ақпараттық қауіпсіздік және ақпаратты қорғау кез келген ұйым немесе мемлекеттің маңызды міндеттерінің бірі болып табылады. Ақпаратты қорғауды қамтамасыз ету үшін заңдар, нормативтік актілер мен стандарттар қабылданған, олар ақпараттық ресурстарды заңсыз қол жеткізуден, бұзудан, ұрлаудан және басқа да зиянды әрекеттерден қорғауға бағытталған. Ақпараттық қауіпсіздікті қорғауға қатысты заңды және нормативтік негіздер келесі маңызды бағыттарды қамтиды: Ұлттық заңдар: әр елде ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданған заңдар мен ережелер бар. Бұл заңдар ақпараттың құпиялылығын, тұтастығын, қолжетімділігін қамтамасыз етуді, сондай-ақ кибершабуылдардың алдын алуды мақсат етеді. Халықаралық стандарттар: әлемдік деңгейде ақпараттық қауіпсіздік саласында бірыңғай стандарттар мен ережелер бар. Олар барлық елдер үшін ортақ қауіпсіздік талаптарын белгілеуге арналған. Халықаралық ұйымдар мен институттар бұл стандарттарды әзірлейді. Нормативтік актілер: ақпараттық қауіпсіздікті қамтамасыз етуге арналған заңға қосымша ережелер мен актілер. Олар ақпараттық жүйелердің қауіпсіздігін қамтамасыз етудің әдістемелік негіздерін анықтайды. Этика және жауапкершілік: ақпаратты қорғау саласындағы заңды актілер тек техникалық шараларды ғана емес, сондай-ақ этикалық нормалар мен жауапкершілікті де қамтиды. Ақпараттық қауіпсіздікке қатысты заңдар жеке тұлғалардың, ұйымдардың және мемлекеттердің құқықтарын, міндеттерін және жауапкершіліктерін реттейді. Ақпараттық қауіпсіздікті қорғауға қатысты халықаралық заңдар мен стандарттар Ақпараттық қауіпсіздікті қорғау саласында халықаралық деңгейде қабылданған бірқатар негізгі заңдар мен стандарттар бар: ISO/IEC 27001 – ақпараттық қауіпсіздікті басқару жүйесінің халықаралық стандарты. Бұл стандарт ақпараттық қауіпсіздік жүйесінің құрылымын, құрылымдық элементтерін, қауіп-қатерлерді басқаруды және жүйенің тиімділігін қамтамасыз етуді қарастырады. GDPR (General Data Protection Regulation) – Еуропалық Одақтың деректерді қорғау жөніндегі жалпы регламенті. Бұл заң жеке деректердің құпиялылығын қорғауды және қолданушылардың деректеріне қатысты құқықтарын қамтамасыз етеді. NIST (National Institute of Standards and Technology) – АҚШ-тағы ақпараттық қауіпсіздік стандарттарын әзірлейтін ұлттық институт. Бұл ұйымның стандарттары әлемде кеңінен қолданылады. COBIT (Control Objectives for Information and Related Technology) – ақпараттық жүйелер мен технологияларды басқару және қауіпсіздік мақсаттары бойынша халықаралық стандарттар мен әдістемелік нұсқаулар. Cybersecurity Framework (CSF) – NIST әзірлеген кіберқорғаныс бойынша стандарт. Бұл құрал ұйымдарға ақпараттық қауіпсіздікті басқаруға арналған басшылықты ұсынады. OECD Guidelines for the Security of Information Systems and Networks – ақпараттық жүйелер мен желілердің қауіпсіздігін қамтамасыз ету бойынша OECD ұсыныстары. Budapest Convention on Cybercrime – киберқылмыспен күрес бойынша халықаралық келісімшарт. Бұл конвенция кибершабуылдарға қарсы іс-шаралар жүргізуге, заңсыз ақпараттық жүйелер мен деректерге қолжетімділікті реттеуге бағытталған. Ақпараттық қауіпсіздікті қорғауға қатысты ұлттық заңдар Әр елде ақпараттық қауіпсіздікті қорғау үшін арнайы заңдар мен нормативтік актілер қабылданған. Қазақстанда ақпараттық қауіпсіздікті қорғауға қатысты бірнеше маңызды заңдар мен ережелер бар: Қазақстан Республикасының «Ақпараттық қауіпсіздік туралы» Заңы: бұл заң ақпараттық қауіпсіздік саласындағы мемлекеттік саясатты, оның міндеттері мен мақсаттарын, сондай-ақ ұлттық қауіпсіздікке қатысты ақпаратты қорғаудың негізгі қағидаттарын белгілейді. Қазақстан Республикасының «Жеке деректер және оларды қорғау туралы» Заңы: жеке тұлғалардың деректерін қорғау, оларды өңдеу және сақтау шарттарын реттейтін заң. Бұл заң ақпараттық жүйелерде жеке деректердің қауіпсіздігін қамтамасыз етуді талап етеді. Қазақстан Республикасының «Электрондық үкімет» Заңы: бұл заң электрондық үкіметті дамыту мен оның қауіпсіздігін қамтамасыз етуге арналған ережелер мен талаптарды белгілейді. Ақпарат және коммуникациялар саласындағы нормативтік актілер: Қазақстанда ақпараттық қауіпсіздікті қамтамасыз ету мақсатында қабылданған түрлі үкіметтік және салалық стандарттар мен ережелер бар. Құқық қорғау органдарының ақпараттық қауіпсіздік бойынша актілері: киберқылмыспен күресу үшін құқық қорғау органдары тарапынан қабылданған заңдар мен ережелер. Ақпараттық қауіпсіздік саясаты мен этика Ақпараттық қауіпсіздікті қорғауға арналған саяси және этикалық талаптар да маңызды. Бұл талаптар ақпараттық қауіпсіздікті қамтамасыз ету кезінде моральдық нормалар мен заңдылықтарды сақтау үшін қажет. Этика мен жауапкершілік: ұйымдар мен жеке тұлғалар ақпараттық жүйелер мен деректерді қорғау бойынша этикалық нормаларды

сақтау керек. Бұл пайдаланушылардың жеке деректерін қорғау, киберқылмыстарды болдырмау, ақпараттық жүйелерді заңсыз пайдалану сияқты мәселелерді қамтиды. Құқықтық жауапкершілік: ақпараттық жүйелерге зиян келтіру, деректерді ұрлау немесе ақпаратты заңсыз өзгерту үшін қылмыстық және азаматтық жауапкершілік қарастырылады.

Бақылау сұрақтары: 1.Ақпараттық қауіпсіздікті қорғауға арналған халықаралық стандарттар мен ережелерді атаңыз. 2.Қазақстан Республикасының «Ақпараттық қауіпсіздік туралы» Заңы қандай міндеттерді қамтиды? 3.ISO/IEC 27001 стандартының ақпараттық қауіпсіздікті басқарудағы маңызы қандай? 4.GDPR (General Data Protection Regulation) қандай құқықтарды қорғайды және оның ақпараттық қауіпсіздікті қорғаудағы рөлі қандай? 5.Ақпараттық қауіпсіздікке қатысты этикалық және құқықтық нормаларды сипаттаңыз.

ДӘРІС №4

Тақырыбы: Ақпараттық қауіптер мен қатерлер. Ақпараттық қауіптер мен қатерлердің түрлері, олардың пайда болу себептері, ықтимал зардаптары.

Ақпараттық қауіптер мен қатерлердің түсінігі Ақпараттық қауіптер және қатерлер — бұл ақпараттық жүйелер мен ресурстарға қауіп төндіретін, оның тұтастығын, құпиялылығын және қолжетімділігін бұзуға бағытталған ықтимал немесе нақты әрекеттер мен жағдайлар. Қауіптер мен қатерлер ақпараттық жүйелердің жұмысын бұзуы немесе зиян келтіруі мүмкін. Қауіп-бұл ақпараттық жүйеге немесе оның құрамдас бөліктеріне зиян келтіру мүмкіндігі. Қауіп жүйенің қауіпсіздігіне төнген нақты қатердің болмауы мүмкін, бірақ жүйе оған бейім болып табылады. Қатер. бұл ақпараттық жүйенің қауіпсіздігіне нақты немесе әлеуетті зиян келтіретін оқиға, әрекет немесе жағдай. Бұл қатердің ықтималдығы жоғары, әрі оның зардаптары елеулі болуы мүмкін. Ақпараттық қауіптер мен қатерлердің тиімді түрде басқарылуы ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін маңызды. Ақпараттық қауіптер мен қатерлердің түрлері Ақпараттық жүйелер мен ресурстарға төнетін қауіптер мен қатерлер әртүрлі болады, оларды мынадай категорияларға бөлуге болады: Физикалық қауіптер: Аптаушылық (Natural Disasters) — табиғи апаттар (жер сілкінісі, су тасқыны, өрт және т.б.) ақпараттық жүйелерге зиян келтіруі мүмкін. Энергетикалық бұзылулар (Power Failures) — жүйенің жұмысын тоқтата алатын электр қуатының үзілуі. Физикалық зиян (Physical Damage) — аппараттық құралдарға (серверлер, компьютерлер) зиян келтіру (мысалы, ұрлау немесе зақымдау). Техникалық қауіптер: Бағдарламалық қателіктер (Software Bugs) — бағдарламалық қамтамасыз етудің ақаулары, жүйенің дұрыс жұмыс істемеуіне немесе ақпараттың бұзылуына әкелуі мүмкін. Жабдық ақаулары (Hardware Failures) — аппараттық құралдардың дұрыс жұмыс істемеуі, мысалы, дисктердің істен шығуы немесе сервердің бұзылуы. Желілік қауіптер: Желілік шабуылдар (Network Attacks) — желі арқылы ақпараттық жүйеге кіруге бағытталған қасақана әрекеттер (мысалы, DoS немесе DDoS шабуылдары). Ақпаратты ұрлау (Data Interception) — ақпараттың заңсыз жолмен көшіру немесе ұрлау әрекеттері. Сегменттеу ақаулары (Segmentation Failures) — жүйенің жеке бөліктерінің арасында шектелген қолжетімділік пен қауіпсіздіктің болмауы. Қолданушылық қауіптер: Адам қателігі (Human Error) — пайдаланушының жүйедегі ақпаратты дұрыс енгізбеуі немесе оның дұрыс емес өңделуі (мысалы, деректердің қателіктері немесе оларды жою). Адамдардың сыртқы әсерлері (Social Engineering) — адамдарды алдау арқылы ақпарат алуға бағытталған әдістер (мысалы, фишинг, телефон алаяқтықтары). Кибершабуылдар: Вирустар және зиянды бағдарламалар (Viruses, Malware) — жүйеге немесе желіге жұққан зиянды бағдарламалар, олар ақпаратты бұзуға, ұрлауға немесе жүйені бақылауға алуға тырысады. Хакерлік шабуылдар (Hacker Attacks) — киберқылмыскерлердің заңсыз жолмен жүйелерге енуі және ақпаратты ұрлауы немесе бұзуы. Фишинг (Phishing) — пайдаланушының жеке деректерін алу үшін қолданылатын алаяқтық әдіс. Ақпараттық жүйелердің ішкі қауіптері: Шығу немесе жариялану (Leaks or Unauthorized Disclosure) — жүйеде сақталған құпия ақпараттың заңсыз немесе рұқсатсыз ашылуы. Деректердің жоғалуы (Data Loss) — ақпараттың толық жойылуы немесе жоғалуы, әсіресе резервтік көшірмелердің болмауы жағдайында. Құқықтық және нормативтік қауіптер: Құқық бұзушылық (Legal Violations) — деректерді қорғау заңдарын бұзу, ақпараттың заңсыз жариялануы немесе сақталмауы. Реттеуші талаптардың бұзылуы (Non-compliance with Regulations) — халықаралық және ұлттық стандарттарға сәйкес келмеу. Ақпараттық қауіптер мен қатерлердің пайда болу себептері Ақпараттық қауіптер мен қатерлердің пайда болуының бірнеше негізгі себептері бар: Техникалық себептер: Жүйе мен жабдықтардың ескіруі немесе дұрыс жұмыс істемеуі. Бағдарламалық қамтамасыз етудің ақаулары немесе қателіктері. Қате конфигурация немесе нашар техникалық қолдау. Адамдық факторлар: Қолданушылардың ақпараттық қауіпсіздік ережелерін сақтамауы (парольді әлсіз таңдау, файлдарды қорғаусыз сақтау). Қателіктер мен жауапсыздық. Әлеуметтік инженерия әдістеріне алданып, қауіпсіздік шараларын бұзу. Киберқылмыскерлердің іс-әрекеттері: Хакерлер мен зиянды бағдарламалар авторларының шабуылдары. Қаржылық немесе саяси мақсатта жасалатын қасақана шабуылдар. Жасанды интеллект пен автоматтандырылған шабуыл құралдарының дамуы. Заңсыз әрекеттер мен реттеудің болмауы: Құқық қорғау мен реттеуші органдардың ақпараттық қауіпсіздік саласындағы талаптарды орындамауы немесе баяулығы. Құпия ақпараттың заңсыз таратылуы. Ақпараттық

қауіптер мен қатерлердің ықтимал зардаптары Ақпараттық қауіптер мен қатерлер ақпараттық жүйелер мен ұйымдарға үлкен зиян келтіруі мүмкін. Олардың ықтимал зардаптары: Ақпараттың жоғалуы немесе бұзылуы: Құпия деректердің жоғалуы немесе ақпараттың бұрмалануы. Заңды немесе басқарушылық шешімдердің дұрыс қабылданбауы. Қаржылық шығындар: Жүйені қалпына келтіруге арналған шығындар. Ұрланған ақпаратты қайта қалпына келтіру немесе қорғау шараларын күшейту үшін қаражат жұмсау. Ұйымның беделінің төмендеуі: Көлік, байланыс немесе бизнес-процестердің бұзылуы нәтижесінде тұтынушылардың сенімінің жоғалуы. Ақпараттық жүйенің қауіпсіздігін бұзатын оқиғалар БАҚ-та жарияланып, ұйымның беделіне зиян келтіруі мүмкін. Құқықтық және нормативтік жазалау: Ақпараттық қауіпсіздік заңдарын бұзу, жеке деректерді қорғауды қамтамасыз етпеу, жүйелік ақаулардың салдарынан құқықтық жауапкершілікке тартылу. Өндірістік және технологиялық тоқтап қалу: Ақпараттық жүйенің бұзылуы немесе тоқтап қалуы нәтижесінде өндірістік процесстердің тоқтап қалу

Бақылау сұрақтары: 1.Ақпараттық қауіптер мен қатерлердің негізгі түрлерін атаңыз. 2.Ақпараттық қауіптер мен қатерлердің пайда болу себептерін сипаттаңыз. 3.Ақпараттық жүйелерге төнетін физикалық қауіптер қандай болуы мүмкін? 4.Кибершабуылдардың қандай түрлері бар және олардың ықтимал зардаптары қандай? 5.Ақпараттық қауіптердің ықтимал зардаптарын атаңыз және олардың алдын алу шараларын түсіндіріңіз.

ДӘРІС №5

Тақырыбы: Шифрлау және криптография негіздері. Ақпаратты қорғаудың негізгі әдістері, шифрлау алгоритмдері, ашық және жабық кілттер, сандық қолтаңбалар.

Шифрлау және криптографияның негізгі түсініктері Криптография — бұл ақпаратты қорғау саласы, оның негізгі мақсаты — ақпаратты рұқсатсыз қолжетімділіктен, бұзудан, өзгертілуден немесе заңсыз жариялануданқорғау. Криптографияның негізінде ақпаратты өзгерту немесе шифрлау арқылы оның тек рұқсат етілген пайдаланушыларға ғана қолжетімді болуын қамтамасыз ету жатады. Шифрлау (encryption) — бұл белгілі бір алгоритм мен кілт арқылы ақпаратты (мәтін немесе деректерді) түсініксіз, шифрланған түрге ауыстыру процесі. Шифрланған ақпарат тек кілтке ие пайдаланушы немесе жүйе арқылы ғана қайта оқуға болады. Дешифрлау (decryption) — бұл шифрланған ақпаратты қайта бастапқы күйіне келтіру процесі, яғни оны оқуға түсінікті ету үшін шифрлау кезінде қолданылған кілттің көмегімен жүзеге асырылады. Ақпаратты қорғаудың негізгі әдістері Ақпаратты қорғаудың бірнеше негізгі әдістері бар: Шифрлау: Ақпаратты рұқсатсыз қолжетімділіктен қорғаудың ең кең таралған әдісі. Шифрлау ақпаратты оқылмайтын түрде ауыстырып, тек құпия кілт арқылы қайтадан бастапқы күйіне келтіруге болады. Цифрлық қолтаңбалар: Құжаттардың немесе хабарламалардың түпнұсқалығын, тұтастығын және авторын тексеруге арналған әдіс. Цифрлық қолтаңба криптографиялық алгоритмдермен қорғалады және оны тек автордың жабық кілті арқылы жасауға болады. Аутентификация: Пайдаланушының немесе жүйенің шынайылығын тексеру процесі. Бұл әдіс парольдер, биометрия, қауіпсіздік сұрақтары және басқа да әдістер арқылы жүзеге асырылады. Хэш-функциялар: Ақпаратты бір жолға ауыстыру және оның тұтастығын тексеру үшін қолданылатын әдіс. Хэш-функциялар ақпараттың қысқаша түсінікті бейнесін (хэш) жасайды, ал бұл хэш бастапқы ақпараттың өзгеріссіздігін бақылауға мүмкіндік береді. Электрондық қолтаңба: Электрондық құжаттарды немесе деректерді заңды түрде тіркеу үшін қолданылады. Бұл да криптографиялық әдіспен жүзеге асырылады, тек ол цифрлық түрде орындалады. Шифрлау алгоритмдері Шифрлау алгоритмдері ақпаратты шифрлаудың әртүрлі тәсілдерін ұсынады. Бұл алгоритмдер ақпаратты сақтау және тасымалдау кезінде оны қорғауға көмектеседі. Симметриялық шифрлау алгоритмдері: Симметриялық шифрлау кезінде ақпаратты шифрлау мен дешифрлауға арналған бір кілт қолданылады. Бұл алгоритмдер өте жылдам, бірақ кілтті қауіпсіз түрде бөлісу қажет. AES (Advanced Encryption Standard) — қазіргі заманғы ең кең таралған симметриялық шифрлау алгоритмі. Ол деректерді 128, 192 және 256 биттік кілттермен шифрлай алады. DES (Data Encryption Standard) — ескі, бірақ әлі де қолданылатын шифрлау алгоритмі. Оның негізгі кемшілігі — кілттің қысқа болуы (56 бит), бұл оны заманауи компьютерлермен бұзу оңай етеді. Асимметриялық шифрлау алгоритмдері: Асимметриялық шифрлау кезінде екі түрлі кілт қолданылады: ашық және жабық. Ашық кілт арқылы ақпарат шифрланады, ал оны тек жабық кілтпен дешифрлауға болады. RSA — ең танымал асимметриялық шифрлау алгоритмі. Бұл алгоритм ашық және жабық кілттерді пайдаланып, деректерді қорғауға арналған. ECC (Elliptic Curve Cryptography) — RSA-ға қарағанда кілттің өлшемі кішірек болғанымен, жоғары қауіпсіздік ұсынады. Ол қазіргі кезде мобильді құрылғылар мен IoT жүйелерінде кеңінен қолданылып келеді. Гибридті шифрлау әдістері: Бұл әдісте симметриялық және асимметриялық шифрлау әдістері біріктіріледі. Мысалы, асимметриялық шифрлау арқылы симметриялық кілт алынады, ал кейінгі деректер осы симметриялық кілтпен шифрланады. Бұл әдіс шифрлау мен дешифрлауды тиімді әрі қауіпсіз етеді. Ашық және жабық кілттер Ашық кілт (Public Key) және жабық кілт (Private Key) — асимметриялық шифрлау жүйесінде қолданылатын екі түрлі кілт. Бұл кілттер бір-бірімен тығыз байланысты, бірақ олар бір-бірін алмастырмайды. Ашық кілт — бұл кілт ақпаратты шифрлау үшін қолданылады. Ол барлық адамдарға қолжетімді болуы мүмкін. Ашық кілтпен

шифрланған деректерді тек жабық кілтпен ғана дешифрлауға болады. Жабық кілт — бұл кілт ақпаратты дешифрлау үшін қолданылады және ол тек оның иесінде ғана болуы керек. Жабық кілтті қауіпсіз сақтау маңызды, өйткені ол тек оның иесіне жүйенің қауіпсіздігі мен аутентификациясын қамтамасыз етеді. Сандық қолтаңбалар Сандық қолтаңба — бұл электронды құжаттың түпнұсқалығы мен тұтастығын тексеру үшін қолданылатын криптографиялық әдіс. Сандық қолтаңба құжаттың авторын анықтауға және оның құжатты өзгеріссіз жібергеніне кепілдік береді. Сандық қолтаңба жасалатын кезде, құжаттың хэш-функциясы есептеліп, оны жабық кілтпен шифрлайды. Қабылдаушы құжатты алған соң, оның хэшін есептеп, ашық кілт арқылы сандық қолтаңбаны тексереді. Егер есептелген хэш сандық қолтаңбаның хэшіне сәйкес келсе, онда құжат өзгертілмеген және оны нақты автор жіберген.

ҚОРЫТЫНДЫ

Ақпаратты қорғау қазіргі заманғы ақпараттық қауіпсіздіктің маңызды бөлігі болып табылады. Шифрлау және криптография әдістері ақпаратты заңсыз қол жеткізуден, бұзудан және ұрлаудан қорғауға көмектеседі. Ашық және жабық кілттер, сандық қолтаңбалар және шифрлау алгоритмдері ақпараттың құпиялылығын және тұтастығын сақтауды қамтамасыз етеді.

Бақылау сұрақтары 1.Криптографияның негізгі мақсаты мен міндеттері қандай? 2.Симметриялық және асимметриялық шифрлау алгоритмдерінің айырмашылықтары қандай? 3.AES және RSA шифрлау алгоритмдерінің ерекшеліктері мен қолданылу салалары қандай? 4.Ашық және жабық кілттерді пайдалану принциптерін түсіндіріңіз. 5.Сандық қолтаңбаның қалай жұмыс істейтінін және оның ақпараттық қауіпсіздік саласындағы рөлін сипаттаңыз.

ДӘРІС №5

Тақырыбы: Компьютерлік вирус және зиянды бағдарламалар. Вирустардың, трояндық бағдарламалардың, шпиондық бағдарламалардың сипаттамасы және олардан қорғану шаралары. Вирус дегеніміз не?

Компьютерлік вирус – бұл өздігінен көбею қабілетіне ие зиянды бағдарлама. Ол басқа бағдарламаларға немесе файлдарға қосылып, солармен бірге таралуы мүмкін. Вирустардың негізгі мақсаты – жүйеде қалыпты жұмыс істейтін бағдарламаларға зақым келтіріп, оларды бұзу немесе жою. Вирустардың түрлері: Файлдық вирустар – бұл вирустар өз кодтарын бағдарламаларға немесе жүйелік файлдарға енгізеді. Олар компьютерді іске қосу кезінде автоматты түрде орындалады. Макровирустар – мәтіндік немесе электрондық кестелер бағдарламаларындағы макрос командаларына еніп, осы құжаттармен бірге таралады. Жүктеу вирустары (Boot sector viruses) – бұл вирустар компьютердің жүктеу секторына енгізіліп, операциялық жүйе жүктелген кезде жұмыс істей бастайды. Трояндық бағдарламалар (Трояндар) дегеніміз не? Трояндық бағдарламалар (трояндар) – бұл сырттай зиянсыз немесе пайдалы болып көрінетін бағдарламалар, бірақ олар компьютерге орнатылған кезде пайдаланушының жеке мәліметтерін ұрлап, жүйеге зиян келтіреді. Олар көбінесе, фишингтік шабуылдар арқылы немесе жалған бағдарламалар ретінде таралады. Трояндардың негізгі белгілері: Пайдаланушының компьютеріне ену үшін ол пайдаланушының өзі орнатуы тиіс. Жасырын түрде жүйенің жұмысын бақылап, мәліметтерді ұрлап немесе басқа зиянды әрекеттер жасайды. Шабуылдаушыға қашықтан басқару мүмкіндігін береді. Шпиондық бағдарламалар (Spyware) дегеніміз не? Шпиондық бағдарламалар – бұл пайдаланушының компьютерін бақылау және оның жеке ақпараттарын жинау мақсатында орнатылатын бағдарламалар. Олар пайдаланушының іс-әрекеттерін бақылап, интернеттегі жүріс-тұрысын тіркейді, сонымен қатар парольдер, төлем мәліметтері мен басқа да жеке деректерді ұрлауы мүмкін. Шпиондық бағдарламалардың функциялары: Жеке ақпаратты жинау (кредиттік карта деректері, логиндер мен парольдер). Пайдаланушының интернет-браузерінде іздеу тарихын бақылау. Пайдаланушының рұқсатынсыз жарнамалық немесе басқа да мазмұндарды көрсету. Компьютердің жұмысын баяулату. Компьютерлік вирустар мен зиянды бағдарламалардан қорғану шаралары Қорғану үшін келесі негізгі шараларды қолдануға болады: Антивирус бағдарламаларын пайдалану: жақсы антивирус бағдарламасы жүйеңізді вирустардан, трояндардан, шпиондық бағдарламалардан қорғауға көмектеседі. Антивирус үнемі жаңартылып отыруы тиіс. Бағдарламаларды және операциялық жүйені жаңарту: Көптеген зиянды бағдарламалар жүйедегі осал жерлерді пайдаланады. Сондықтан бағдарламалық жасақтаманы, операциялық жүйені үнемі жаңартып отыру маңызды. Желілік қауіпсіздік: құпия сөздерді күрделі етіп жасау, жеке деректерді тек сенімді веб-сайттарда енгізу және интернетте тексерілмеген немесе күмәнді сілтемелерге баспау қажет. Фишингтен сақтану: Пайдаланушыға жалған электрондық

хаттар немесе веб-сайттар арқылы шабуыл жасалуы мүмкін. Сондықтан электрондық хаттардағы сілтемелерге абай болу керек. Қосымша қауіпсіздік қабаттарын қосу: Мысалы, екі факторлы аутентификация, шифрлау және брандмауэрді қолдану.

ҚОРЫТЫНДЫ:

Компьютерлік вирус және зиянды бағдарламалар қазіргі кезде кең таралған қауіптердің бірі. Олар компьютерлік жүйелерді зақымдап, жеке мәліметтерді ұрлап, қолданушылардың қаржылық және жеке қауіпсіздігіне қауіп төндіреді. Осы себепті, вирустар мен зиянды бағдарламалардан қорғану шараларын сақтау өте маңызды. Бұл үшін антивирус бағдарламалары мен жүйелік қауіпсіздік шараларын үнемі жаңартып, қолданушының өз әрекеттерін қадағалау қажет.

Бақылау сұрақтары: 1.Компьютерлік вирус дегеніміз не? Олардың қандай негізгі түрлері бар? 2.Трояндық бағдарламалардың негізгі ерекшеліктері қандай? 3.Шпиондық бағдарламалар қандай мақсатта қолданылады? Олардың негізгі функциялары қандай? 4.Вирустар мен зиянды бағдарламалардан қорғану үшін қандай негізгі шаралар қолданылуы керек? 5.Фишинг дегеніміз не және оған қарсы қандай сақтық шараларын қолдану қажет?

ДӘРІС №6

Тақырыбы: Желілік қауіпсіздік. Желілік шабуылдар, фишинг, DoS және DDoS шабуылдары, firewalldep мен IDS/IPS жүйелерінің рөлі.

Желілік қауіпсіздік Желілік қауіпсіздік — бұл ақпараттық жүйелер мен желілерді қорғаудың жиынтығы, оның ішінде деректердің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету мақсатында қолданылатын шаралар мен технологиялар. Желілік қауіпсіздіктің басты мақсаты — желілік ресурстарды қорғау және жүйедегі ақпаратты зиянды әрекеттерден сақтау. Желілік шабуылдар Желілік шабуылдар-бұл киберқылмыскерлердің компьютерлік желілерді бұзу, деректерді ұрлау немесе жүйелерді зақымдау мақсатында жасайтын әрекеттері. Желілік шабуылдар әр түрлі түрлерге бөлінеді, олардың әрқайсысы өзінде әр түрлі технологияларды қолдана отырып, түрлі тәсілдермен іске асырылады. Желілік шабуылдардың түрлері: Белсенді шабуылдар — шабуылдаушы жүйенің жұмысын бұзып, оны өзгертуге немесе жоюға бағытталған шабуылдар. Пассивті шабуылдар- желі арқылы мәліметтерді ұрлау немесе тыңдау мақсатында жасалады, жүйеге зиян келтірмейді. Фишинг (Phishing) Фишинг - бұл пайдаланушыны алаяқтыққа түсіру арқылы жеке ақпараттарды (құпия сөздер, қаржылық деректер) ұрлау үшін қолданылатын әдіс. Әдетте, фишинг шабуылдары электрондық пошта немесе фальшивті веб-сайттар арқылы жүзеге асырылады. Пайдаланушы жалған хабарламаларға немесе сайттарға сілтемелерді басқанда, шабуылдаушылар олардың құпия деректерін жинап алады. Фишингтің ерекшеліктері: Жалған хабарламалар немесе веб-сайттар арқылы жеке мәліметтерді жинау. Электрондық пошталарда сенімді ұйымдардың атауын қолдану. Сайттардың URL мекен-жайлары мен атауларын ұқсастырып жазу. DoS және DDoS шабуылдары DoS (Denial of Service) — қызметтен бас тарту шабуылы. Бұл шабуыл жүйенің немесе желінің қызметтерін тоқтату немесе бұзу үшін жүзеге асырылады. DoS шабуылы кезінде шабуылдаушы үлкен көлемде артық сұраныстар жіберу арқылы жүйенің ресурстарын сарқып тастайды, нәтижесінде жүйе жұмыс істемей қалуы мүмкін. DoS шабуылдарының түрлері: Flooding (су тасқыны): Желіні немесе серверді қажетсіз сұраныстармен толтырып, жүйенің жұмысын тоқтатады. Protocol attacks: Желілік хаттамалардағы осалдықтарды пайдалану арқылы қызметті тоқтату. DDoS (Distributed Denial of Service) — таратылған қызметтен бас тарту шабуылы. Бұл шабуылдың түрі DoS шабуылынан ерекшеленеді, себебі ол бірнеше компьютердің немесе сервердің бір мезгілде бірігіп жасайтын шабуылы болып табылады. DDoS шабуылы кезінде шабуылдаушылар түрлі ботнеттерді (зиянды бағдарламалар арқылы бақылауға алынған мыңдаған құрылғылар) пайдаланады. DoS және DDoS шабуылдарының айырмашылығы: DoS: бір компьютер арқылы жасалады. DDoS: көптеген құрылғылардан (ботнет) бір уақытта жасалады. Firewall (Қорғаныс брандмауэры) Firewall (Қорғаныс брандмауэры)-бұл желілік қауіпсіздікті қамтамасыз ету үшін қолданылатын құрылғы немесе бағдарламалық қамтамасыз ету, ол ішкі желімен сыртқы желі арасындағы трафикті бақылап, сұраныстарды сүзеді. Firewall жүйе мен желі арасындағы қорғаныс қабаты ретінде жұмыс істейді. Firewall қызметтері: Трафикті фильтрациялау: желіге кіруге немесе шығуға болатын деректер пакеттерін реттейді. Қауіпсіздік саясатын жүзеге асыру: әртүрлі ережелер негізінде трафикті рұқсат етілген немесе тыйым салынған етіп бөледі. Вирустар мен зиянды бағдарламалардан қорғану үшін сүзгілер қолдану. IDS/IPS жүйелері IDS (Intrusion Detection System) — Басқыншылықты анықтау жүйесі — желіге немесе жүйеге шабуыл жасаған кезде бұл жүйелер қауіп-қатерлерді анықтап, әкімшілерге ескерту жасайды. IDS негізінен шабуылдың болғанын белгілейді, бірақ олар оған қарсы әрекет етпейді. IPS (Intrusion Prevention System) — Басқыншылықты болдырмау жүйесі — IDS жүйесімен салыстырғанда, IPS жүйесі тек қауіп-қатерлерді анықтап қана

қоймай, оларға дереу қарсы әрекет жасайды (мысалы, трафикті тоқтату немесе фильтрациялау). IDS/IPS жүйелерінің рөлі: IDS- шабуылдарды анықтап, ескерту береді. IPS-— шабуылдардың алдын алып, оларды болдырмайды. Қауіп-қатерлерді дер кезінде анықтап, жүйе қауіпсіздігін қамтамасыз етеді.

ҚОРЫТЫНДЫ

Желілік қауіпсіздік — ұйымның немесе жеке тұлғаның ақпараттық қауіпсіздігін сақтау үшін маңызды аспект болып табылады. Қазіргі уақытта кибершабуылдар барған сайын күрделене түсуде, сондықтан желіні қорғау үшін заманауи құралдар мен технологияларды қолдану өте маңызды. DoS және DDoS шабуылдары, фишинг және басқа зиянды әрекеттердің алдын алу үшін желілік қауіпсіздік құралдары (firewall, IDS/IPS жүйелері) тиімді жұмыс істеуі қажет.

Бақылау сұрақтары: 1.Желілік шабуылдардың қандай түрлері бар және олардың айырмашылығы неде? 2.Фишинг дегеніміз не? Оның белгілері мен қорғану жолдары қандай? 3.DoS және DDoS шабуылдарының айырмашылығы неде? 4.Firewall қандай қызмет атқарады және оның желілік қауіпсіздік жүйесіндегі рөлі қандай? 5.IDS және IPS жүйелерінің жұмыс принципі мен айырмашылығы неде? Конец формы

ДӘРІС №7

Тақырыбы: Ақпараттық жүйелерді қорғаудың техникалық құралдары.≣ Антивирус бағдарламалары, firewall жүйелері, шифрлау құралдары және олардың қолдану әдістері.

Ақпараттық жүйелерді қорғаудың техникалық құралдары

Ақпараттық жүйелерді қорғау- ақпараттық қауіпсіздікті қамтамасыз ету, деректерді қорғау және жүйенің тұтастығын сақтау мақсатында қолданылатын әртүрлі техникалық құралдар мен әдістердің кешені. Бұл құралдар жүйені сыртқы және ішкі қауіптерден қорғауға, жүйедегі ақпаратты ұрлап кетуден, бұзудан немесе зақымдаудан сақтауға бағытталған. Ақпараттық жүйелерді қорғаудың техникалық құралдарына келесілер кіреді: Антивирус бағдарламалары Firewall жүйелері Шифрлау құралдары Антивирус бағдарламалары Антивирус бағдарламалары- бұл компьютерді вирус, трояндық бағдарламалар, шпиондық бағдарламалар және басқа зиянды бағдарламалардан қорғауға арналған бағдарламалар. Олар жүйеге енетін вирустар мен зиянды кодтарды анықтап, жоюға немесе оларды оқшаулауға мүмкіндік береді. Антивирус бағдарламаларының негізгі функциялары: Вирус анықтау: антивирус бағдарламалары белгілі бір зиянды бағдарламаларды анықтап, оларды жүйеден жояды немесе оқшаулайды. Вирустарды (worm), трояндық бағдарламаларды (trojan), шпиондық бағдарламаларды (spyware) анықтау: антивирус жүйесі компьютерде орнатылған бағдарламалардың арасында зиянды бағдарламаларды іздеп, оларды анықтайды. Вирустық базаны жаңарту: жаңа вирустар мен зиянды бағдарламалар үнемі пайда болады, сондықтан антивирус бағдарламасы вирустық базасын жиі жаңартып отыруы қажет. Жүйені сканерлеу: антивирус жүйесі пайдаланушыға компьютерді толығымен немесе оның бөліктерін сканерлеу арқылы зиянды бағдарламаларды табуға мүмкіндік береді. Қолдану әдістері: Реал уақыттық қорғау: антивирус бағдарламасы жүйенің жұмысын тоқтатпай, оның артында автоматты түрде жұмыс істейді, жаңа файлдар немесе бағдарламалар жүйеге қосылғанда оларды тексереді. Қолмен сканерлеу: Пайдаланушы қажет болған жағдайда белгілі бір файлды немесе бүкіл жүйені тексереді. Жаңартулар: антивирус бағдарламасын үнемі жаңартып отыру қажет, өйткені жаңа вирустар үнемі пайда болады. Firewall (Қорғаныс брандмауэры) Firewall (қорғаныс брандмауэры) — бұл желіаралық қорғау құрылғысы немесе бағдарламасы, ол жүйе мен сыртқы желі арасында келетін және кететін деректер пакеттерін фильтрациялап, жүйеге зиянды трафиктің енуіне жол бермейді. Firewall жүйесінің негізгі функциялары: Қорғаныс ережелерін орнату: Пайдаланушы желі арқылы кіретін және шығатын деректер пакеттерін сүзгіден өткізу үшін ережелер орнатады. Трафикті бақылау: Желідегі барлық кіріс және шығыс трафикті бақылайды. Бұл шара желіге кіруге немесе шығуға болатын деректерді анықтап, талапқа сай болмаса оларды бұғаттайды. Қауіпсіздік хаттамаларын іске қосу: брандмауэр жүйесі желі қауіпсіздігін сақтау үшін белгілі бір хаттамалар мен порттарды пайдалану немесе шектеу қою арқылы жұмыс істейді. Қолдану әдістері: Кеңселік желілерде: құрылғыларды бір-бірінен және сыртқы интернет желісінен қорғаныс қабаты арқылы бөліп, трафикті сүзу. Интернет желісінде: Интернетке қосылған әрбір құрылғыны қорғау, соның ішінде үйлесімді антивирус бағдарламаларымен және шифрлау құралдарымен біріктіру. Шифрлау құралдары Шифрлау — бұл ақпаратты қорғау әдісі, яғни деректерді тек белгілі бір кілтпен немесе құпия сөзбен оқуға болатын кодталған формаға айналдыру. Шифрлау жүйелері деректерді қауіпсіз түрде тасымалдауға, сақтау мен пайдалануға мүмкіндік береді. Шифрлаудың негізгі түрлері: Симметриялық шифрлау: Бұл жағдайда шифрлау және дешифрлау үшін бір кілт пайдаланылады. Құпия кілтті сақтай білу маңызды, өйткені оны жоғалтқан жағдайда деректерді қайтадан қалпына келтіру мүмкін болмайды. Асимметриялық шифрлау: Бұл шифрлауда екі кілт пайдаланылады: біреуі

деректерді шифрлау үшін, екіншісі оларды дешифрлау үшін. Әдетте, бұл тәсіл көп қолданылатын электронды пошта мен қауіпсіз байланыс жүйелерінде пайдаланылады. Шифрлау құралдарының қолдану әдістері: Ақпаратты сақтау кезінде шифрлау: Мысалы, сыртқы қатты дискілердегі деректерді немесе қалталарды шифрлау арқылы оларды ұрлау немесе заңсыз қол жеткізуге қарсы қорғау. Ақпаратты тасымалдау кезінде шифрлау: Желі арқылы ақпарат тасымалдағанда (мысалы, HTTPS, VPN) шифрлау арқылы деректердің құпиялылығын сақтау. Электрондық хаттарды шифрлау: Электрондық пошта арқылы жіберілетін ақпаратты шифрлау, әсіресе құпия деректермен жұмыс істейтін компаниялар үшін өте маңызды.

ҚОРЫТЫНДЫ

Ақпараттық жүйелерді қорғау үшін техникалық құралдарды қолдану — бұл ұйымның немесе жеке тұлғаның деректерін және жүйелерін зиянды бағдарламалардан, желілік шабуылдардан және басқа да қауіптерден қорғаудың маңызды аспектісі. Антивирус бағдарламалары, firewall жүйелері және шифрлау құралдары ақпараттық қауіпсіздікті қамтамасыз ету үшін өте тиімді және қажетті құралдар болып табылады.

Бақылау сұрақтары: 1.Антивирус бағдарламаларының қандай негізгі функциялары бар және оларды қалай қолдануға болады? 2.Firewall жүйесінің негізгі жұмыс принципі қандай? Оның қолдану әдістерін түсіндіріңіз. 3.Шифрлау дегеніміз не? Шифрлаудың қандай түрлері бар және оларды қайда қолдануға болады? 4.Шифрлау құралдарын қолдану кезінде қандай қауіпсіздік шараларын сақтау керек? 5.Антивирус бағдарламалары мен firewall жүйелерінің арасындағы айырмашылықтарды түсіндіріңіз. Конец формы

ДӘРІС № 8

Тақырыбы: Ақпараттық қауіпсіздік бойынша аудит және мониторинг.
Ақпараттық жүйелердің қауіпсіздігін бақылау, тексеру және анализ жүргізу. Аудит жүйелері мен логтарды өңдеу. Ақпараттық қауіпсіздік бойынша аудит және мониторинг

Ақпараттық қауіпсіздік бойынша аудит және мониторинг — бұл ақпараттық жүйелер мен желілердің қауіпсіздігін қамтамасыз ету үшін қолданылатын маңызды шаралар мен әдістер. Олар жүйелердің тұтастығын, құпиялылығын және қолжетімділігін бақылау мақсатында жүргізіледі. Ақпараттық жүйелердің қауіпсіздігін тексеру мен талдау жүйелі түрде жүргізіледі, ал аудит және мониторинг — бұл жүйедегі қауіпсіздік саясатын бағалау және оны жақсартуға бағытталған шаралар кешені. Ақпараттық жүйелердің қауіпсіздігін бақылау Ақпараттық қауіпсіздік бақылауы- бұл жүйенің жұмысын бақылау, оқиғаларды тіркеу, аномалияларды анықтау және жүйенің қауіпсіздік деңгейін тексеру үдерісі. Ол жүйеге қатысты тәуекелдерді бағалауға және сол тәуекелдерден туындайтын қауіптерді анықтауға мүмкіндік береді. Бақылаудың негізгі бағыттары: Жүйе мен желі трафигін бақылау: Желідегі аномалды әрекеттер мен трафикті мониторингтеу, шабуылдарды анықтау. Қолданушылардың әрекеттерін бақылау: Пайдаланушының жүйеде жасаған әрекеттерін бақылап, олардың рұқсатсыз әрекеттерін анықтау. Қауіпсіздік бұзушылықтарын анықтау: Жүйеде орын алған немесе орын алуы мүмкін қауіпсіздік инциденттерін бақылау және талдау.

Бақылаудың құралдары: Желілік мониторинг құралдары: Желідегі трафикті бақылауға және аномалияларды анықтауға арналған құралдар. Мысалы, Wireshark, Snort. Қолданушы әрекеттерін бақылау жүйелері: Қолданушының жүйеде жасаған барлық әрекеттерін жазып алатын жүйелер. Мысалы, SIEM (Security Information and Event Management) құралдары. Ақпараттық қауіпсіздік бойынша аудит Ақпараттық қауіпсіздік аудиті -бұл ұйымның ақпараттық жүйелерінің қауіпсіздігін тексеру, оның ақаулары мен осалдықтарын анықтау және ұйымның қауіпсіздік саясатына сәйкестігін бағалау үдерісі. Аудит, әдетте, сыртқы тәуелсіз аудиторлар тарапынан немесе ұйымның ішкі қауіпсіздік бөлімінің көмегімен жүзеге асырылады. Аудиттің негізгі кезеңдері: Дайындық кезеңі: Аудиторлық тексеру жүргізу үшін нақты мақсаттар мен ауқымды анықтау. Талдау кезеңі: Жүйе компоненттерін, қауіпсіздік саясатын және ішкі бақылау жүйелерін тексеру. Есеп беру кезеңі: Аудит нәтижелерін қорытындылау және қауіпсіздік шараларын жақсартуға ұсыныстар беру. Аудиттің негізгі бағыттары: Қолданушылардың рұқсаттарын тексеру: Әрбір қолданушының қолжетімділігі мен құқықтарын тексеру. Жүйелік қорғаныс деңгейін бағалау: Желідегі қауіпсіздік шараларын, жүйелік патчтарды және аутентификация тәсілдерін тексеру. Шабуылға қарсы қорғаныс қабаттарын бағалау: Желілік қорғау құралдарының, антивирус бағдарламаларының, firewall жүйелерінің тиімділігін бағалау. Логтарды өңдеу және анализ Логтарды өңдеу-бұл жүйеде орын алған оқиғалар мен әрекеттердің жазбаларын (логтарын) жинақтап, талдау үдерісі. Логтар жүйе туралы ақпараттың маңызды көзі болып табылады және олардың дұрыс өңделуі ақпараттық қауіпсіздік саласындағы маңызды аспект болып табылады. Логтарды өңдеудің мақсаты: Қауіпсіздік инциденттерін анықтау: Логтар арқылы жүйеге жасалған шабуылдарды немесе басқа да

қауіпсіздік бұзушылықтарын анықтау. Жүйелік ақауларды табу: жүйедегі ақауларды, жүйенің дұрыс жұмыс істемеуін анықтау. Мониторинг және бақылау: пайдаланушылардың әрекеттерін және жүйенің жұмысын бақылау. Логтарды талдау құралдары: SIEM жүйелері: Логтар мен оқиғаларды жинақтап, талдап, шабуылдарды анықтауға көмектесетін құралдар. Мысалы, Splunk, ELK Stack. Қолданушы әрекеттерін бақылау құралдары: Пайдаланушының жүйедегі әртүрлі әрекеттерін жазып алып, оларды тексеру және талдау үшін қолданылады. Аномалияларды анықтау құралдары: Логтарды талдай отырып, жүйедегі күдікті немесе аномалды әрекеттерді анықтауға арналған құралдар. Логтарды өңдеу әдістері: Логтарды жинау: Барлық жүйелік, желілік және қолданушылық оқиғалардың жазбаларын жинақтау. Логтарды өңдеу және талдау: Логтар арқылы жүйеде орын алған оқиғаларды талдап, олардың заңдылығын тексеру. Ескерту және есеп беру: Логтардан алынған нәтижелер негізінде қауіпсіздік бұзушылықтары немесе күдікті әрекеттер туралы есептер жасау.

ҚОРЫТЫНДЫ

Ақпараттық қауіпсіздік аудиті мен мониторингін жүйелі түрде жүргізу — бұл ақпараттық жүйенің қауіпсіздігін қамтамасыз ету үшін маңызды құрал. Аудит және мониторинг жүйенің әлсіз тұстарын анықтауға, қауіпсіздік бұзушылықтарын ерте кезеңде анықтауға және жүйенің қорғанысын жақсартуға мүмкіндік береді. Логтарды өңдеу мен талдау қауіпсіздік инциденттерін анықтау мен жүйенің тұтастығын тексерудің тиімді әдісі болып табылады.

Бақылау сұрақтары: 1.Ақпараттық жүйелердің қауіпсіздігін бақылау мен тексеру дегеніміз не? Ол үшін қандай негізгі әдістер қолданылады? 2.Ақпараттық қауіпсіздік аудитінің негізгі кезеңдері мен мақсаттары қандай? 3.Логтарды өңдеу мен талдаудың негізгі мақсаттары қандай және ол қандай құралдармен жүзеге асырылады? 4.SIEM жүйелері мен олардың ақпараттық қауіпсіздік саласындағы рөлі қандай? 5.Ақпараттық жүйелердің қауіпсіздігін бағалағанда қандай қауіптер мен ақауларды анықтау маңызды?

ДӘРІС № 9

Тақырыбы: Ішкі және сыртқы қауіптерден қорғау әдістері. Қызметкерлердің қателіктері, әлеуметтік инженерия, сыртқы шабуылдардан қорғану шаралары.

Ақпараттық қауіпсіздік бойынша аудит және мониторинг Ақпараттық қауіпсіздік бойынша аудит және мониторинг- бұл ақпараттық жүйелер мен желілердің қауіпсіздігін қамтамасыз ету үшін қолданылатын маңызды шаралар мен әдістер. Олар жүйелердің тұтастығын, құпиялылығын және қолжетімділігін бақылау мақсатында жүргізіледі. Ақпараттық жүйелердің қауіпсіздігін тексеру мен талдау жүйелі түрде жүргізіледі, ал аудит және мониторинг — бұл жүйедегі қауіпсіздік саясатын бағалау және оны жақсартуға бағытталған шаралар кешені. Ақпараттық жүйелердің қауіпсіздігін бақылау Ақпараттық қауіпсіздік бақылауы — бұл жүйенің жұмысын бақылау, оқиғаларды тіркеу, аномалияларды анықтау және жүйенің қауіпсіздік деңгейін тексеру үдерісі. Ол жүйеге қатысты тәуекелдерді бағалауға және сол тәуекелдерден туындайтын қауіптерді анықтауға мүмкіндік береді. Бақылаудың негізгі бағыттары: Жүйе мен желі трафигін бақылау: Желідегі аномалды әрекеттер мен трафикті мониторингтеу, шабуылдарды анықтау. Қолданушылардың әрекеттерін бақылау: пайдаланушының жүйеде жасаған әрекеттерін бақылап, олардың рұқсатсыз әрекеттерін анықтау. Қауіпсіздік бұзушылықтарын анықтау: жүйеде орын алған немесе орын алуы мүмкін қауіпсіздік инциденттерін бақылау және талдау. Бақылаудың құралдары: Желілік мониторинг құралдары: Желідегі трафикті бақылауға және аномалияларды анықтауға арналған құралдар. Мысалы, Wireshark, Snort. Қолданушы әрекеттерін бақылау жүйелері: қолданушының жүйеде жасаған барлық әрекеттерін жазып алатын жүйелер. Мысалы, SIEM (Security Information and Event Management) құралдары. Ақпараттық қауіпсіздік бойынша аудит Ақпараттық қауіпсіздік аудиті-бұл ұйымның ақпараттық жүйелерінің қауіпсіздігін тексеру, оның ақаулары мен осалдықтарын анықтау және ұйымның қауіпсіздік саясатына сәйкестігін бағалау үдерісі. Аудит, әдетте, сыртқы тәуелсіз аудиторлар тарапынан немесе ұйымның ішкі қауіпсіздік бөлімінің көмегімен жүзеге асырылады. Аудиттің негізгі кезеңдері: Дайындық кезеңі: Аудиторлық тексеру жүргізу үшін нақты мақсаттар мен ауқымды анықтау. Талдау кезеңі: жүйе компоненттерін, қауіпсіздік саясатын және ішкі бақылау жүйелерін тексеру. Есеп беру кезеңі: аудит нәтижелерін қорытындылау және қауіпсіздік шараларын жақсартуға ұсыныстар беру. Аудиттің негізгі бағыттары: Қолданушылардың рұқсаттарын тексеру: әрбір қолданушының қолжетімділігі мен құқықтарын тексеру. Жүйелік қорғаныс деңгейін бағалау: Желідегі қауіпсіздік шараларын, жүйелік патчтарды және аутентификация тәсілдерін тексеру. Шабуылға қарсы қорғаныс қабаттарын бағалау: желілік қорғау құралдарының, антивирус бағдарламаларының, firewall жүйелерінің тиімділігін бағалау. Логтарды өңдеу және анализ Логтарды өңдеу - бұл жүйеде орын алған оқиғалар мен әрекеттердің жазбаларын (логтарын) жинақтап, талдау үдерісі. Логтар жүйе туралы ақпараттың маңызды көзі болып табылады және олардың дұрыс өңделуі ақпараттық қауіпсіздік саласындағы маңызды аспект болып табылады. Логтарды

өңдеудің мақсаты: Қауіпсіздік инциденттерін анықтау: логтар арқылы жүйеге жасалған шабуылдарды немесе басқа да қауіпсіздік бұзушылықтарын анықтау. Жүйелік ақауларды табу: жүйедегі ақауларды, жүйенің дұрыс жұмыс істемеуін анықтау. Мониторинг және бақылау: Пайдаланушылардың әрекеттерін және жүйенің жұмысын бақылау. Логтарды талдау құралдары: SIEM жүйелері: Логтар мен оқиғаларды жинақтап, талдап, шабуылдарды анықтауға көмектесетін құралдар. Мысалы, Splunk, ELK Stack. Қолданушы әрекеттерін бақылау құралдары: Пайдаланушының жүйедегі әртүрлі әрекеттерін жазып алып, оларды тексеру және талдау үшін қолданылады. Аномалияларды анықтау құралдары: логтарды талдай отырып, жүйедегі күдікті немесе аномалды әрекеттерді анықтауға арналған құралдар. Логтарды өңдеу әдістері: Логтарды жинау: Барлық жүйелік, желілік және қолданушылық оқиғалардың жазбаларын жинақтау. Логтарды өңдеу және талдау: логтар арқылы жүйеде орын алған оқиғаларды талдап, олардың заңдылығын тексеру. Ескерту және есеп беру: Логтардан алынған нәтижелер негізінде қауіпсіздік бұзушылықтары немесе күдікті әрекеттер туралы есептер жасау.

ҚОРЫТЫНДЫ

Ақпараттық қауіпсіздік аудиті мен мониторингін жүйелі түрде жүргізу — бұл ақпараттық жүйенің қауіпсіздігін қамтамасыз ету үшін маңызды құрал. Аудит және мониторинг жүйенің әлсіз тұстарын анықтауға, қауіпсіздік бұзушылықтарын ерте кезеңде анықтауға және жүйенің қорғанысын жақсартуға мүмкіндік береді. Логтарды өңдеу мен талдау қауіпсіздік инциденттерін анықтау мен жүйенің тұтастығын тексерудің тиімді әдісі болып табылады. Ішкі және сыртқы қауіптерден қорғау әдістері Ақпараттық жүйелер мен желілердің қауіпсіздігін қамтамасыз ету — бұл кешенді процесс, ол ішкі және сыртқы қауіптерді анықтау, алдын алу және олардан қорғауды қамтиды. Қауіптер әр түрлі көздерден туындауы мүмкін, сондықтан оларды ескеріп, тиісті қорғау шараларын қолдану өте маңызды. Ішкі қауіптерден қорғау Ішкі қауіптер - бұл жүйеге немесе желіге ұйым ішінде орналасқан адамдардың немесе қызметкерлердің тарапынан төнетін қауіптер. Мұндай қауіптер әдетте қызметкерлердің қателіктері, қасақана зиян келтіру немесе әлеуметтік инженерия әдістерін қолданумен байланысты болуы мүмкін. Қызметкерлердің қателіктері: Қызметкерлердің қателіктері -ішкі қауіптердің ең көп тараған түрлерінің бірі. Олар әдетте адамдық факторға байланысты туындайды және әдетте назар аудармау, қауіпсіздік шараларын сақтамау, немесе қауіпті әрекеттерді білместен жасау арқылы пайда болады. Қызметкерлердің қателіктері мыналар болуы мүмкін: Құпия ақпаратты дұрыс сақтамау. Құпия сөздерді әлсіз немесе жалпыға қолжетімді ету. Вирустар мен зиянды бағдарламалардан қорғайтын құралдарды қолданбау. Электрондық пошта арқылы фишингтік шабуылдармен байланысқа түсу. Құпия ақпаратты рұқсатсыз бөлісу немесе тасымалдау. Қызметкерлерді қорғау әдістері: Қауіпсіздік оқыту: Қызметкерлерді ақпараттық қауіпсіздік туралы оқыту, фишинг шабуылдары, әлеуметтік инженерия әдістері және дұрыс қауіпсіздік саясатын сақтау маңызды. Құпия сөздер мен аутентификация: қызметкерлерге қауіпсіз құпия сөздер қолдануды талап ету және екі факторлы аутентификацияны енгізу. Қолданушының құқықтарын шектеу: әр қызметкерге тек оның жұмысына қажетті деректер мен жүйелерге ғана қолжетімділікті беру. Бұл минималды принципке сәйкес келеді. Мониторинг және бақылау: қызметкерлердің жүйедегі әрекеттерін бақылау, әсіресе құпия деректерге қол жеткізу кезінде. Әлеуметтік инженерия (Social Engineering) Әлеуметтік инженерия - бұл адамдарды сендіру арқылы ақпаратты ұрлау немесе жүйеге қол жеткізуге қолайлы жағдай жасау әдісі. Бұл әдіс әдетте технологиялық қорғанысты бұзып, адамның сеніміне кіріп, маңызды мәліметтерді немесе жүйелерді ұрлауға бағытталған. Әлеуметтік инженерия әдістеріне мыналар жатады: Фишинг: электрондық пошта немесе жалған веб-сайттар арқылы қолданушының құпия деректерін ұрлау. Смишинг (SMS фишинг): Мобильді құрылғылар арқылы фишингтік шабуыл жасау. Вишинг (Voice phishing): Телефон арқылы адамдарды алдап, құпия ақпаратты алу. Претекстинг: Жалған ақпаратты ұсыну арқылы пайдаланушылардан қажетті деректерді алу. Бейтаныс тұлғаларға сенім арттыру: қауіпсіздік шараларын бұзу үшін адамды алдау немесе манипуляция жасау. Әлеуметтік инженериядан қорғану шаралары: Қызметкерлерді оқыту: әлеуметтік инженерия шабуылдары туралы қызметкерлерге ақпарат беру. Құпия ақпаратты тексеру: Егер күмәнді сұраулар немесе өтініштер болса, оларды қосымша тексеруден өткізу. Қауіпсіздік саясаттарын енгізу: құпия деректер мен ақпаратты сұрауға арналған заңды әдістерді ғана қолдануды талап ету. Сыртқы шабуылдардан қорғану Сыртқы шабуылдар-бұл кибершабуылдардың түрлері, олар сыртқы тараптардан (хакерлер, киберқылмыскерлер, ұйымдар немесе үкіметтік құрылымдар) жүзеге асырылады. Бұл шабуылдар желі немесе жүйе арқылы өтетін деректерді ұрлауға, бұзуға немесе жүйеге кіруге бағытталған. Сыртқы шабуылдардың негізгі түрлері: DoS және DDoS шабуылдары: Қызметтен бас тарту шабуылдары- бұл жүйені немесе желіні үлкен көлемдегі сұраныстармен толтыру арқылы оның қызметін тоқтату. SQL инъекциясы: Веб-сайттар мен дерекқорларға зиянды код енгізу арқылы мәліметтерді ұрлау немесе жүйені бұзу. Cross-Site Scripting (XSS): Веб-браузерлерде орындалатын зиянды скрипттерді енгізу арқылы ақпаратты ұрлау. Malware (Зиянды бағдарламалар): Вирус, троян, шпиондық бағдарламалар мен басқа да зиянды кодтар жүйеге ену үшін қолданылады. Man-in-the-middle шабуылы: деректерді жіберу кезінде оларды ұрлау немесе өзгерту мақсатында пайдаланушы мен сервер арасында шабуыл жасау. Сыртқы шабуылдардан қорғану шаралары: Брандмауэр және антивирус бағдарламалары: желілік трафикті бақылап, зиянды бағдарламаларды анықтау үшін брандмауэр мен антивирус бағдарламаларын қолдану. Жүйені шифрлау: құпия деректерді тасымалдау кезінде

шифрлау әдістерін қолдану (мысалы, SSL/TLS). Ақпараттық жүйелерді жаңарту: қауіпсіздік жаңартуларын және патчтарды уақытында орнату, осалдықтарды жою. VPN қолдану: Қашықтан жұмыс істейтін қызметкерлер үшін VPN арқылы қауіпсіз байланыс орнату. Көпфакторлы аутентификация: қолданушылардың жүйеге кіруін қосымша тексеру үшін екі немесе көп факторлы аутентификация қолдану.

ҚОРЫТЫНДЫ

Ішкі және сыртқы қауіптерден қорғану үшін кешенді шаралар қолдану қажет. Қызметкерлердің қателіктерінен, әлеуметтік инженериядан және сыртқы шабуылдардан қорғану үшін қауіпсіздік мәдениетін қалыптастыру, тиісті техникалық құралдарды енгізу және жүйелік бақылау жүргізу маңызды.

Бақылау сұрақтары: 1.Қызметкерлердің қателіктерінен қорғау үшін қандай шаралар қолдануға болады? 2.Әлеуметтік инженерияның негізгі әдістері қандай? Оларға қарсы қалай қорғануға болады? 3.Сыртқы шабуылдардан қорғану үшін қандай құралдар мен әдістер қолданылуы қажет? 4.SQL инъекциясы мен XSS шабуылдары туралы айтып беріңіз. Оларға қарсы қандай қорғаныс шараларын қолдануға болады? 5.Әлеуметтік инженерияға қарсы қызметкерлерді оқыту қандай маңызды аспектілерді қамтуы тиіс?

ДӘРІС № 10

Тақырыбы: Бұлтты есептеу орталықтарындағы қауіпсіздік. Бұлтты қызметтердің қауіпсіздігі, деректерді сақтау және басқару, қызмет көрсетуші тараптан қауіпсіздікті қамтамасыз ету.

Ақпараттық қауіпсіздік бойынша аудит және мониторинг Ақпараттық қауіпсіздік бойынша аудит және мониторинг - бұл ұйымның ақпараттық жүйелерінің қауіпсіздігін қамтамасыз ету және оларды үнемі бақылап отыру процесі. Мұның мақсаты — жүйенің қауіпсіздігін тексеру, әлеуетті қауіптерді анықтау, сондай-ақ жүйе мен деректердің қолжетімділігін, тұтастығын және құпиялылығын сақтау. Ақпараттық жүйелердің қауіпсіздігін бақылау Ақпараттық жүйелердің қауіпсіздігін бақылау — бұл ұйымның ақпараттық жүйелерінде қауіпсіздік талаптарының сақталуын қамтамасыз ету үшін жүргізілетін жүйелі әрекеттер мен процестер жиынтығы. Қауіпсіздік бақылау жүйелерінің мақсаты — қауіптерді уақытында анықтап, жүйеге қауіп төндіретін әрекеттерді болдырмау. Бақылау шараларының негізгі элементтері: Қолданушы әрекеттерін бақылау: Қолданушылардың жүйеде орын алған әрекеттері, олардың жүйеге қолжетімділігі мен операцияларын тексеру. Бұл ақпаратты жүйе әкімшілері жүйелік журналдарда сақтайды. Келетін және шығатын трафикті бақылау: желі трафигін бақылау арқылы ұйымның қауіпсіздік бұзушылықтарын анықтауға болады. Антивирус және брандмауэрлерді қолдану: антивирус бағдарламалары мен брандмауэрлерді қолдану, шабуылдардың алдын алу және жүйеге заңсыз кіру әрекеттерін бақылау. Ақпараттық жүйелерді тексеру және анализ жүргізу Ақпараттық жүйелердің қауіпсіздігін тексеру және анализ жүргізу- бұл жүйедегі кемшіліктерді анықтап, оларды жақсарту шараларын ұсыну процесі. Бұл тексеру екі түрге бөлінеді: Аудит және тестілеу: Жүйелердің осалдықтарын тексеру (vulnerability scanning): Ақпараттық жүйелерді осалдықтарға тексеру үшін арнайы құралдар мен бағдарламалар пайдаланылады. Бұл жүйенің сыртқы және ішкі осалдықтарын анықтауға көмектеседі. Пенетралдық тестілеу (penetration testing): жүйенің қауіпсіздігін тексерудің белсенді әдісі болып табылады. Тест жүргізушілер жүйеге заңсыз кіруге тырысып, кемшіліктерді анықтайды. Қауіпсіздік аудиті: ақпараттық жүйелер мен процестердің сәйкесін тексеру. Аудиторлар ұйымның қауіпсіздік саясатын, процедураларын, және қолданатын техникалық шешімдерін бағалайды. Талдау және есеп беру: Логтарды талдау: қауіпсіздік оқиғаларын тіркеу үшін қолданылатын лог файлдары мен жүйелік журналдарды талдау. Бұл әрекет жүйедегі күдікті әрекеттер мен ақауларды анықтауға мүмкіндік береді. Қауіпсіздік саясатын талдау: ұйымның ақпараттық қауіпсіздік саясатының іске асырылуын және оның тиімділігін тексеру. Бұл кезеңде қызметкерлердің қауіпсіздік тәртібі мен олардың іс-әрекеттері тексеріледі. Аудит жүйелері мен логтарды өңдеу Ақпараттық жүйелерде орын алған оқиғалар мен әрекеттерді тіркеу үшін лог файлдары маңызды рөл атқарады. Логтарды өңдеу — бұл жүйелердің әрекеттерін қадағалау, күдікті әрекеттерді анықтау, және заңсыз әрекеттерді тіркеу үшін жүргізілетін үдеріс. Логтарды өңдеудің негізгі кезеңдері: Логтарды жинау: Барлық жүйелер мен құрылғылардан лог файлдарын жинау. Лог файлдары әртүрлі ақпаратты қамтиды, мысалы, қолданушы әрекеттері, жүйе күйі, желі трафигі және т.б. Логтарды талдау: логтарды мұқият талдай отырып, күдікті немесе заңсыз әрекеттерді анықтау. Бұл үдеріс жүйе әкімшілеріне жүйедегі қауіпті оқиғаларды уақтылы табуға мүмкіндік береді. Бақылау құралдарын пайдалану: логтарды өңдеу үшін автоматтандырылған құралдарды пайдалану. Мысалы, SIEM (Security Information and Event Management) жүйелерін қолдану, олар оқиғаларды тіркеп, талдайды. Есеп беру: логтарды талдағаннан кейін, қауіпсіздік оқиғалары туралы есептер жасау. Бұл есептер ұйымның қауіпсіздік деңгейін жақсартуға арналған шараларды анықтауға көмектеседі.

ҚОРЫТЫНДЫ: АҚПАРАТТЫҚ ҚАУІПСІЗДІК АУДИТІ МЕН МОНИТОРИНГІНІҢ МАҢЫЗДЫЛЫҒЫ – ҰЙЫМНЫҢ АҚПАРАТТЫҚ ЖҮЙЕЛЕРІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ, ДЕРЕКТЕРДІ ҚОРҒАУ, ЖӘНЕ ЖҮЙЕЛЕРДІҢ ТҰТАСТЫҒЫН САҚТАУ. БҰЛ ҮДЕРІСТЕР ҰЙЫМНЫҢ ІШКІ ЖӘНЕ СЫРТҚЫ ҚАУІПТЕРГЕ ҚАРСЫ ШАРАЛАРЫН ЖЕТІЛДІРУГЕ ЖӘНЕ АЛДЫН АЛУҒА МҮМКІНДІК БЕРЕДІ. ЛОГТАРДЫ ӨҢДЕУ ЖӘНЕ ЖҮЙЕЛЕРДІ ТАЛДАУ БАРЫСЫНДА АНЫҚТАЛҒАН ӘЛСІЗДІКТЕР МЕН ҚАУІПТЕРГЕ УАҚЫТЫНДА ЖАУАП БЕРУ – ТИІМДІ ҚАУІПСІЗДІК ЖҮЙЕСІНІҢ НЕГІЗІ.

Бақылау сұрақтары: 1.Ақпараттық жүйелердің қауіпсіздігін бақылаудың негізгі шаралары қандай? 2.Ақпараттық жүйелерді тексеру мен анализ жүргізу кезінде қандай негізгі әдістер қолданылады? 3.Пенетралдық тестілеу мен осалдықтарды тексеру арасындағы айырмашылықты түсіндіріңіз. 4.Логтарды өңдеу процесінің негізгі кезеңдерін сипаттаңыз. 5.Ақпараттық қауіпсіздік аудиті қандай мақсатты көздейді және ол қалай жүзеге асырылады? Конец формы

ДӘРІС № 11

Тақырыбы: Ішкі және сыртқы қауіптерден қорғау әдістері. Қызметкерлердің қателіктері, әлеуметтік инженерия, сыртқы шабуылдардан қорғану шаралары. Ішкі және сыртқы қауіптерден қорғау әдістері:

Қызметкерлердің қателіктерінен қорғану шаралары: Қызметкерлердің қателіктері ақпараттық қауіпсіздікке үлкен қатер төндіреді. Бұл қателіктер көбінесе жұмыс кезінде абайсыздықтан, білім жетіспеушілігінен, немесе жеке қателіктерден туындайды. Сондықтан қызметкерлерді қорғаудың негізгі шаралары: Оқыту және тренингтер: қызметкерлерді ақпараттық қауіпсіздік бойынша үздіксіз оқыту. Бұл олардың фишинг (қолданушының деректерін алдау арқылы), вирус, және басқа да қауіптерден хабардар болуын қамтамасыз етеді. Қауіпсіздік процедураларын енгізу: мысалы, паролдерді күрделі етіп жасау, екі факторлы аутентификация (2FA) қолдану және мәліметтерді дұрыс сақтау. Қызметкерлердің қолжетімділігін шектеу: тек қажетті ақпаратқа ғана қолжетімділік беру (немесе минималды рұқсат принципі). Әлеуметтік инженериядан қорғану әдістері: әлеуметтік инженерия - адамның психологиясын пайдалану арқылы қауіпсіздік жүйелерін айналып өту әдісі. Бұл әдіс адамдарды манипуляциялау немесе олардың сенімін алдап пайдалану арқылы шабуыл жасалады. Оқытуды және хабардар етуді қамтамасыз ету: қызметкерлерге әлеуметтік инженерияның әдістері туралы үйрету, олардың алданып қалмауы үшін, телефонымен және электрондық пошта арқылы белгісіз адамдардан келген сұраныстарға абай болуды ескерту. Фишингке қарсы қорғау: электрондық пошта арқылы фишинг шабуылдарына қарсы шараларды күшейту. Мысалы, белгісіз сілтемелерді немесе тіркемелерді ашпау туралы ескерту. Құпия ақпаратты қорғау: Құпия деректерді тексеруден өтпеген адамдармен бөлісуден аулақ болу, мәліметтерді дұрыс сақтау. Сыртқы шабуылдардан қорғану әдістері: сыртқы шабуылдар-бұл хакерлердің немесе басқа сыртқы тұлғалардың жүйелер мен желілерге заңсыз кіру әрекеттері. Бұл шабуылдар көбінесе желіге, серверлерге, және құрылғыларға бағытталады. Қауіпсіздік қабаттарын енгізу: қабатталған қауіпсіздік шаралары қолдану, мысалы, брандмауэрлер, антивирус бағдарламалары, және қосымша аутентификация жүйелері. Шифрлау: мәліметтерді шифрлау ақпараттың қауіпсіздігін қамтамасыз етеді, яғни егер олар сыртқы шабуылдан ұрланған жағдайда, оларды оқу мүмкін болмайды. Желілік мониторинг: жүйеде қалыпты емес әрекеттерді анықтау үшін үздіксіз желілік мониторинг жүргізу. Жаңартулар мен патчтарды уақытында орнату: бағдарламалық қамтамасыз етудің жаңартуларын уақытында орнату арқылы қауіптерді азайту. Құпия деректерді қорғау: құпия деректердің сақталуы мен қорғалуы — ақпараттық қауіпсіздік саласындағы маңызды аспектілердің бірі. Бұл деректердің заңсыз қолжетімділіктен немесе ұрлықтан қорғауын қамтиды. Деректерді шифрлау: Құпия деректерді сақтау және беру кезінде шифрлау әдістерін қолдану. Бұл ақпаратты тек заңды пайдаланушылар ғана оқи алатын етіп қорғайды. Құпия ақпараттың физикалық қауіпсіздігі: құжаттар мен құрылғыларды тек рұқсат етілген тұлғаларға қолжетімді ету. Мысалы, құжаттарды құлыппен жабу немесе компьютерлердің физикалық қауіпсіздігін қамтамасыз ету. Қолданушы рұқсаттарын басқару: деректерге қолжетімділікті нақты адамдар мен қызметкерлердің міндеттері мен қажеттіліктеріне сәйкес шектеу. Бұл «минималды рұқсат» принципін сақтау арқылы жүзеге асырылады. Операциялық жүйелер мен бағдарламалық қамтамасыз ету қауіпсіздігі: жүйе мен қосымшалардың қауіпсіздігі олардың жұмыс істеуіндегі маңызды қорғаныс қабатын құрайды. Қосымшалар мен операциялық жүйелердің дұрыс конфигурациялануы және жаңартуларының уақытында орнатылуы ақпараттық қауіпсіздікті күшейтеді. Бағдарламалық қамтамасыз етуді жаңарту: операциялық жүйе мен қосымшаларды үнемі жаңарту және патчтар орнату — қауіпті алаңдарды жабуға көмектеседі. Қосымшаларды тексеру: қауіпсіздік тексерулері мен аудиттерін жүйелі түрде

өткізу, әсіресе ашық бастапқы кодты қосымшаларды пайдалану кезінде. Қауіпсіздік протоколдарын пайдалану: SSL/TLS сияқты қауіпсіздік хаттамаларын қолдану арқылы мәліметтерді қорғау. Кибершабуылдарға қарсы қорғаныс және инциденттерге жауап беру: кибершабуылдарға және ақпараттық қауіпсіздік инциденттеріне дер кезінде және дұрыс жауап беру өте маңызды. Бұл ұйымды жүйелі түрде қорғау үшін маңызды қадам болып табылады. Кибершабуылдарға дайындық жоспары: қауіпсіздік инциденттерін алдын ала болжау және оларды басқаруға арналған жоспар құру. Инциденттерді бақылау және тіркеу: қауіпсіздік бұзушылықтары мен күмәнді әрекеттерді тіркеп, оларды тексеру және тиісті шараларды қабылдау. Тез арада жауап беру және қалпына келтіру: инциденттер кезінде жүйелерді қалпына келтіру және қауіпсіздікті қалпына келтіру үшін дереу әрекет ету.

ҚОРЫТЫНДЫ: ІШКІ ЖӘНЕ СЫРТҚЫ ҚАУІПТЕРДЕН ҚОРҒАНУ ҰЙЫМНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН КӨПТЕГЕН ТӘСІЛДЕРДІ БІРІКТІРУДІ ТАЛАП ЕТЕДІ. ОЛАРҒА ҚЫЗМЕТКЕРЛЕРДІ ОҚЫТУ, ӘЛЕУМЕТТІК ИНЖЕНЕРИЯДАН ҚОРҒАУ, СЫРТҚЫ ШАБУЫЛДАРДАН САҚТАНУ, ДЕРЕКТЕРДІ ҚОРҒАУ, ЖҮЙЕЛЕРДІ ҚАУІПСІЗ ЕТУ ЖӘНЕ КИБЕРШАБУЫЛДАРҒА ДАЙЫН БОЛУ КІРЕДІ. ҚАУІПСІЗДІК ШАРАЛАРЫНЫҢ ТИІМДІ БОЛУЫ ҰЙЫМНЫҢ АҚПАРАТТЫҚ РЕСУРСТАРЫ МЕН ДЕРЕКТЕРІНІҢ САҚТАЛУЫНА ЖӘНЕ ҚҰҚЫҚТЫҚ ТАЛАПТАРҒА СӘЙКЕСТІГІН ҚАМТАМАСЫЗ ЕТЕДІ.

Бақылау сұрақтары: 1.Қызметкерлердің ақпараттық қауіпсіздікке әсер ететін негізгі қателіктерін атаңыз және олардан қалай қорғануға болады? 2.Әлеуметтік инженерияның қандай түрлері бар және одан қорғану үшін қандай шаралар қолдануға болады? 3.Сыртқы шабуылдардың түрлерін атаңыз және олардан қорғану үшін қандай әдістерді пайдалануға болады? 4.Қызметкерлерге ақпараттық қауіпсіздік бойынша қандай оқыту бағдарламаларын ұсынар едіңіз? Желі қауіпсіздігін қамтамасыз ету үшін қолданылатын негізгі шараларды сипаттаңыз.

ДӘРІС № 12

Тақырыбы: Бұлтты есептеу орталықтарындағы қауіпсіздік. Бұлтты қызметтердің қауіпсіздігі, деректерді сақтау және басқару, қызмет көрсетуші тараптан қауіпсіздікті қамтамасыз ету. Бұлтты есептеу орталықтарындағы қауіпсіздік

Бұлтты есептеу (Cloud Computing) дегеніміз не? Бұлтты есептеу — бұл қызмет көрсетуші тараптан инфрақұрылым, платформалар мен бағдарламалар түріндегі ресурстарды интернет арқылы пайдалануға мүмкіндік беретін технология. Бұл технология пайдаланушыларға ресурстарды арендаға алу, масштабтауға және қажет болған жағдайда олардың көлемін арттыру немесе азайту мүмкіндігін береді. Бұлтты есептеу орталықтарындағы қауіпсіздіктің маңызы Бұлтты есептеу орталықтарында қауіпсіздік мәселелері өте маңызды болып табылады, себебі бұлтты қызметтер түрлі ұйымдардың мәліметтерін сақтайды, олардың жұмысының үздіксіздігіне жауапты болады және жеке ақпараттардың қорғалуын қамтамасыз етеді. Бұлтты орталықтарындағы қауіпсіздік келесі аспектілерді қамтиды: Құпиялылық: деректердің ұрлануын немесе бұзылуын болдырмау. Бұл үшін деректер шифрлануы және қолжетімділік деңгейі бойынша саясаттар қабылданады. Қолжетімділік: бұлттық ресурстарға қолжетімділіктің үнемі сақталуы қажет. Қауіпсіздік жүйелері үзіліссіз жұмыс істеуге кепілдік береді. Тұтастық (Integrity): деректердің бүтіндігін сақтау. Қолданушыларға және қызмет көрсетушіге деректердің дұрыс күйін қамтамасыз ету керек. Аутентификация және авторизация: пайдаланушылардың кім екенін тексеру (аутентификация) және оларды тиісті қызметтерге (ресурстарға) кіргізу (авторизация). Бұлтты қызметтердің қауіпсіздігі Бұлтты қызметтерді пайдалану барысында келесі қауіпсіздік шараларын ескеру қажет: Шифрлау: бұлттағы деректерді шифрлау – деректердің бұзылуы немесе ұрлануы жағдайында оларды оқуға болмайтын формада сақтау. Қолданушы қолжетімділігін басқару: қолданушылардың жүйеге кіру құқықтарын басқару, рұқсатсыз кіруді болдырмау. Көпфакторлы аутентификация: қолданушыны тексерудің бірнеше тәсілі (пароль, SMS арқылы код алу, биометрия). Мониторинг және журнал жүргізу: қызметтерді пайдалану кезінде орын алатын әрбір әрекетті бақылау және тіркеу. Қауіпсіздік стандарттары мен сәйкестіктер: ISO 27001, GDPR сияқты қауіпсіздік стандарттары мен құқықтық талаптарды орындау. Деректерді сақтау және басқару Бұлтта деректерді сақтау мен басқару кезінде бірнеше маңызды аспектілер ескеріледі: деректердің сақталуы: бұлтты есептеу орталықтарындағы деректер серверлерде немесе арнайы құрылғыларда сақталады, олар белгілі бір жерде физикалық түрде орналасуы мүмкін, бірақ оларды қашықтан қол жеткізу

арқылы пайдалану жеңілдейді. Деректердің резервтік көшірмесін жасау: деректерді жоғалту немесе зақымданудан қорғау үшін резервтік көшірмелерді сақтау. Құпиялылық пен заңнамалық талаптар: деректердің қай жерде сақталуы, қандай заңдар мен ережелер бойынша өңделетіні – бұл да маңызды аспектілер. Қызмет көрсетуші тараптан қауіпсіздікті қамтамасыз ету Қызмет көрсетуші тараптың қауіпсіздікті қамтамасыз ету жауапкершілігі: Физикалық қауіпсіздік: Бұлттық серверлер мен құрылғылардың физикалық қауіпсіздігін қамтамасыз ету. Серверлік және желілік қауіпсіздік: Желідегі қауіпсіздік, firewall орнату, кіріс және шығыс трафигін бақылау. Қызмет көрсету деңгейіндегі келісімшарттар (SLA): қызмет көрсетуші тараптың ұсынатын қауіпсіздік шаралары мен кепілдіктері. Шифрлау және деректерді қорғау: деректерді қорғаудың техникалық шаралары. Қызмет көрсету үзілістерінің алдын алу: сервистің үздіксіз жұмыс істеуін қамтамасыз ету және апаттық жағдайлар үшін дайындық.

Бақылау сұрақтары: 1.Бұлтты есептеу қызметтерінде қауіпсіздік пен құпиялылықты қалай қамтамасыз етуге болады? 2.Бұлтты есептеу орталықтарында деректерді сақтаудың қандай қауіптері бар және оларды қалай болдырмауға болады? 3.Қызмет көрсетуші тараптың бұлтты қызметтердегі қауіпсіздікті қамтамасыз етудегі міндеттері қандай? 4.Шифрлау әдістерінің бұлтты есептеу орталықтарындағы маңызы қандай? 5.Қолданушылардың жүйеге кіру құқығын басқару үшін қандай шаралар қолданылуы тиіс?

ДӘРІС № 13

Тақырыбы: Интернеттегі қауіпсіздік Интернет арқылы берілетін мәліметтердің қауіпсіздігі, веб-сайттардың қорғау шаралары, SSL/TLS сертификаттары

Интернеттегі қауіпсіздік Интернеттегі қауіпсіздік - бұл интернет арқылы алмасатын мәліметтердің қорғалуы, ақпараттың тұтастығы, құпиялылығы және қолжетімділігін қамтамасыз ету мақсатындағы шаралар мен әдістердің жиынтығы. Интернеттегі қауіпсіздік мәліметтерді сақтау, жеткізу және өңдеу кезінде қорғау шараларын қолдануды талап етеді. Интернет арқылы берілетін мәліметтердің қауіпсіздігі Интернет арқылы мәліметтерді беру кезінде ақпарат қауіпсіздігіне қауіп төндіретін бірнеше фактор бар. Бұл мәліметтерді ұрлау, өзгерту, немесе олардың дұрыс емес жолмен пайдаланылуы мүмкін. Сондықтан мәліметтердің қауіпсіздігін қамтамасыз ету үшін түрлі шаралар қолданылады. Мәліметтердің қауіпсіздігі шаралары: Шифрлау (Encryption): мәліметтерді шифрлау — бұл ақпаратты тек рұқсат етілген тұлғалар ғана оқи алатындай етіп өзгерту процесі. Интернет арқылы өтетін мәліметтерді шифрлау ақпараттың сыртқы шабуылдардан немесе ұрлықтан қорғалуының басты әдісі болып табылады. Құпиялылық: құпия ақпаратты қорғау үшін шифрлаудан басқа әдістер де қолданылады, мысалы, жеке куәліктер мен қаржылық деректерді дұрыс сақтау және оларды тек шектелген тұлғаларға ұсыну. Қауіпсіздік хаттамалары: HTTPS, SSL/TLS сияқты қауіпсіздік хаттамалары арқылы мәліметтердің Интернетте берілгенде сақталуын қамтамасыз ету. Веб-сайттардың қорғау шаралары Веб-сайттардың қауіпсіздігін қорғау үшін бірнеше негізгі шаралар қолданылады. Бұл шаралар веб-сайттарды зиянды шабуылдардан, хакерлердің заңсыз әрекеттерінен және зиянды бағдарламалардан қорғауды көздейді. Веб-сайттарды қорғау шаралары: SSL/TLS сертификаттары: Веб-сайттарда пайдаланылатын SSL/TLS сертификаттары мәліметтерді шифрлау арқылы веб-сайтқа кірген қолданушының деректерін қорғауға көмектеседі. Қауіпсіздіктің тұрақты жаңартылуы: Веб-сайттар мен қосымшалардың қауіпсіздігін үнемі тексеріп, жаңартып отыру қажет. Бұл негізінен қауіпсіздік жаңартуларын және патчтарын уақтылы орнатуды білдіреді. SQL инъекцияларынан қорғану: SQL инъекциялары — веб-сайттарға шабуыл жасау үшін пайдаланылатын кең тараған әдіс. Бұл шабуылдардан қорғану үшін веб-сайттың бағдарламалық коды қауіпсіздікті қамтамасыз етуі керек. Құпия сөздерді қорғау: Веб-сайттарда қолданушылардың паролін қорғау үшін күшейтілген шифрлау әдістерін қолдану қажет. Сондай-ақ, парольдер мен аутентификация жүйелерінің қауіпсіздігін қамтамасыз ету маңызды. SSL/TLS сертификаттары SSL (Secure Sockets Layer) және TLS (Transport Layer Security) — бұл мәліметтерді интернет арқылы жіберген кезде олардың қауіпсіздігін қамтамасыз ететін криптографиялық протоколдар. SSL/TLS сертификаттары веб-сайттың қауіпсіздігі мен қолданушының деректерін қорғауға арналған. SSL/TLS сертификаттарының негізгі ерекшеліктері: Шифрлау: SSL/TLS сертификаттары веб-сайт пен оның қолданушысы арасындағы барлық мәліметтерді шифрлайды, сондықтан мәліметтерді бөгде тұлғалар оқи алмайды. Деректердің тұтастығы: SSL/TLS сертификаттары мәліметтердің тасымалдау кезінде өзгермейтіндігіне кепілдік береді. Бұл ақпараттың тұтастығын сақтауға көмектеседі. Аутентификация: SSL/TLS сертификаттары веб-сайттың шынайы екенін және оның пайдаланушыға қауіпсіз екенін тексереді, яғни фишингтік шабуылдардан қорғайды. HTTPS: SSL/TLS сертификаттары веб-сайттың мекен-жайын HTTPS протоколы арқылы көрсетуге мүмкіндік береді. HTTPS — бұл HTTP протоколының қауіпсіз нұсқасы, онда мәліметтер шифрланып жіберіледі. SSL/TLS сертификаттарының түрлері: Domain Validation (DV): бұл сертификаттар тек веб-сайттың доменін тексереді және ең қарапайым түрі болып табылады.

Organization Validation (OV): бұл сертификаттар веб-сайттың иесінің аты-жөнін тексереді, сонымен бірге оның қауіпсіздігін қамтамасыз етеді. Extended Validation (EV): бұл ең сенімді сертификат болып табылады, себебі ол веб-сайттың заңдығын терең тексеруді талап етеді.

ҚОРЫТЫНДЫ: ИНТЕРНЕТТЕГІ ҚАУІПСІЗДІК — АҚПАРАТТЫ ҚОРҒАУДЫҢ МАҢЫЗДЫ ЭЛЕМЕНТІ БОЛЫП ТАБЫЛАДЫ. ИНТЕРНЕТ АРҚЫЛЫ МӘЛІМЕТТЕРДІ ШИФРЛАУ, SSL/TLS СЕРТИФИКАТТАРЫ ЖӘНЕ ВЕБ-САЙТТАРДЫҢ ҚОРҒАУ ШАРАЛАРЫ — БҰЛ ПАЙДАЛАНУШЫЛАРДЫҢ ДЕРЕКТЕРІН ҚОРҒАУДЫҢ НЕГІЗГІ ҚҰРАЛДАРЫ. ИНТЕРНЕТТЕГІ ҚАУІПСІЗДІКТІ САҚТАУ ҮШІН ШИФРЛАУ, ҚАУІПСІЗДІК ХАТТАМАЛАРЫН ҚОЛДАНУ ЖӘНЕ ВЕБ-САЙТТАРДЫҢ ҚАУІПСІЗДІГІН ҮНЕМІ БАҚЫЛАП ОТЫРУ ӨТЕ МАҢЫЗДЫ.

Бақылау сұрақтары: 1.Интернет арқылы берілетін мәліметтердің қауіпсіздігін қамтамасыз ету үшін қандай шаралар қолданылуы керек? 2.Веб-сайттарды қорғау үшін қандай негізгі шаралар қажет? 3.SSL/TLS сертификаттарының мақсаты мен негізгі ерекшеліктерін түсіндіріңіз. 4.SSL және TLS арасындағы айырмашылықты сипаттаңыз. 5.Веб-сайттың қауіпсіздігін тексеру кезінде қандай техникалық шаралар қолдануға болады?

ДӘРІС № 14

Тақырыбы: Бизнес пен ақпараттық қауіпсіздіктің интеграциясы. Ақпараттық қауіпсіздікті бизнес процесстерімен біріктіру, тәуекелдерді басқару, ұйымдық қауіпсіздік стратегиялары.

Бизнес пен ақпараттық қауіпсіздіктің интеграциясы Ақпараттық қауіпсіздік қазіргі таңда тек технологиялық және техникалық аспектілермен шектелмейді, ол бизнес стратегияларының маңызды бөлігіне айналды. Әрбір ұйым үшін ақпараттық қауіпсіздік оның бизнес мақсаттарына жетуге көмектесетін және оларды қорғайтын маңызды құралы болып табылады. Бизнес пен ақпараттық қауіпсіздіктің интеграциясы — бұл қауіптерді тиімді басқару, бизнес процесстерін қорғау және ұйымның ақпараттық активтерін қорғау үшін қажетті шараларды біріктіру үдерісі. Ақпараттық қауіпсіздікті бизнес процесстерімен біріктіру Ақпараттық қауіпсіздік стратегиясын ұйымның жалпы бизнес стратегиясымен біріктіру -қауіптерді басқарудың тиімді жолы болып табылады. Бизнес мақсаттарына жету барысында ақпараттық қауіпсіздік талаптары мен қағидаттарын ескеру керек, себебі ақпараттық қауіпсіздіктің бұзылуы ұйымның беделіне, қаржылық жағдайына және заңды міндеттемелеріне зиян келтіруі мүмкін. Ақпараттық қауіпсіздіктің бизнес процестермен интеграциясы: Ақпараттық қауіпсіздік мақсаттарын бизнес мақсаттарымен сәйкестендіру: бизнес стратегиясының құрамдас бөлігі ретінде ақпараттық қауіпсіздіктің мақсаттарын анықтап, оларды бизнес процестерінде қолдану. Мысалы, қаржылық операцияларды жүргізу кезінде ақпараттың қауіпсіздігін сақтау. Ақпараттық қауіпсіздік саясаттарының бизнес процесстеріне әсері: ақпараттық қауіпсіздікке қатысты саясатиен қабылданатын шешімдер бизнес процестеріне әсер етуі тиіс. Мысалы, клиенттік деректерді қорғау саясаты — сату және маркетинг стратегияларына ықпал етуі мүмкін. Қауіпсіздік стандарттарын енгізу: ақпараттық қауіпсіздік стандарттарын бизнес процестеріне интеграциялау (ISO 27001, NIST және т.б.) арқылы ұйымдағы ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету. Тәуекелдерді басқару Ақпараттық қауіпсіздіктің басты мақсаты- ұйымның ақпараттық ресурстарын қорғау және тәуекелдерді басқару болып табылады. Тәуекелдерді басқару — бұл қауіпті жағдайлар мен ықтимал қауіптерді алдын ала анықтау және оларды азайту немесе басқару үдерісі. Тәуекелдерді басқарудың негізгі кезеңдері: Тәуекелді бағалау: Әрбір бизнес процесте ықтимал қауіптерді анықтап, оларды бағалау. Бұл кезеңде қауіптер мен тәуекелдер бойынша нақты деректер жинау және оларды жүйелі түрде талдау маңызды. Тәуекелді азайту шаралары: тәуекелдерді басқару стратегиясы қауіпті жағдайлардың ықтималдығын азайтуға бағытталған шараларды қамтиды. Мысалы, шифрлау әдістерін қолдану, резервтік көшірмелер жасау, немесе желілік қауіпсіздікті күшейту. Тәуекелдерді бақылау және қайта қарау: тәуекелдерді басқару үдерісі үнемі жаңартылып, өзгертілуі тиіс. Бұл ұйымдағы қауіптерді жаңа технологиялар мен жағдайларға сәйкес бақылап отыруды қамтиды. Ұйымдық қауіпсіздік стратегиялары Ұйымның ақпараттық қауіпсіздік стратегиялары - бұл ұйымның ақпараттық қауіпсіздік талаптарына сай әрекет етуіне мүмкіндік беретін жоспарлар мен бағыттар. Стратегиялар ұйымның ұзақ мерзімді мақсаттарына жету үшін ақпараттық қауіпсіздік шараларын тиімді іске асыруды қамтамасыз етеді. Ұйымдық қауіпсіздік стратегияларын құру кезінде ескерілетін негізгі аспектілер: Қауіпсіздіктің барлық деңгейде қамтамасыз етілуі: ұйымның ақпараттық қауіпсіздігі барлық деңгейде, яғни жоғарғы басқарудан бастап, операциялық деңгейлерге дейін

қамтамасыз етілуі тиіс. Бұл барлық қызметкерлер мен бөлімшелердің ақпараттық қауіпсіздікке жауапкершілігін арттырады. Ақпараттық қауіпсіздік мәдениетін дамыту: қызметкерлердің ақпараттық қауіпсіздікке деген жауапкершілігін арттыру үшін ұйым ішінде ақпараттық қауіпсіздік мәдениетін қалыптастыру өте маңызды. Технологиялық және физикалық қорғаныс шараларының бірігуі: ақпараттық қауіпсіздік стратегиясында тек техникалық қорғау шаралары емес, сондай-ақ физикалық қауіпсіздік шаралары да болуы керек. Мысалы, физикалық қауіпсіздік - сервер бөлмелеріне қолжетімділік шектеулері. Шығындарды және қауіптерді бағалау: қауіпсіздік стратегиялары қаржылық және құқықтық шығындардың алдын алуға бағытталуы тиіс. Бұл стратегиялар тәуекелдерді азайту арқылы ұйымның шығындарын үнемдеуге көмектеседі.

ҚОРЫТЫНДЫ

Ақпараттық қауіпсіздік пен бизнес процестерін интеграциялау қазіргі заманғы ұйымдар үшін өте маңызды. Ақпараттық қауіпсіздік стратегиясын бизнес мақсаттарына сәйкес құру және тәуекелдерді басқару арқылы ұйым өзінің ресурстарын қорғап, қауіптерді минимизациялайды. Осылайша, бизнес пен ақпараттық қауіпсіздіктің үйлесімді түрде жұмыс істеуі ұйымның жетістігі мен қауіпсіздігіне оң әсерін тигізеді.

Бақылау сұрақтары: 1.Ақпараттық қауіпсіздікті бизнес процестеріне интеграциялау үшін қандай негізгі шаралар қолданылуы қажет? 2.Тәуекелдерді басқарудың негізгі кезеңдерін сипаттаңыз. 3.Ақпараттық қауіпсіздік стратегиясын құру кезінде қандай факторлар ескерілуі керек? 4.Ұйымдағы ақпараттық қауіпсіздіктің мәдениетін дамыту үшін қандай шараларды қолдануға болады? 5.Ақпараттық қауіпсіздік пен бизнес стратегияларының үйлесімділігі ұйым үшін қандай артықшылықтар береді?

ДӘРІС № 15

Тақырыбы: Ақпараттық қауіпсіздік саласындағы болашақ трендтер. Жасанды интеллект, блокчейн және басқа жаңа технологиялардың ақпараттық қауіпсіздікке әсері. Ақпараттық қауіпсіздік саласындағы болашақ трендтер

Ақпараттық қауіпсіздік саласы үнемі өзгеріп, жаңарып отырады, себебі жаңа технологиялар мен тұжырымдамалар пайда болады. Бұл өзгерістер ұйымдардың қауіпсіздік стратегиялары мен шешімдерін жетілдіруге ықпал етеді. Қазіргі уақытта жасанды интеллект, блокчейн және басқа жаңа технологиялар ақпараттық қауіпсіздікке терең әсер етуде. Бұл технологиялар ақпараттық қауіпсіздік саласын қалай өзгертетінін, қандай жаңа мүмкіндіктер ашатындығын және қандай тәуекелдермен бірге келетінін түсіну маңызды. Жасанды интеллект (AI) және машиналық оқыту (ML) Жасанды интеллект және машиналық оқыту қазіргі ақпараттық қауіпсіздік жүйелерін түбегейлі өзгертуі мүмкін. Бұл технологиялар қауіптерді болжау, шабуылдарды автоматты түрде анықтау және оларға қарсы әрекет ету үшін қолданылады. Атап айтқанда, AI мен ML жүйелері деректерді талдай отырып, шабуылдардың паттерндерін үйреніп, оларды алдын ала анықтауға көмектеседі.

Жасанды интеллекттің ақпараттық қауіпсіздікке әсері: Шабуылдарды алдын алу: AI мен ML жүйелері зиянды әрекеттердің белгілерін анықтауға және шабуылдарды алдын ала болжауға қабілетті. Бұл жүйелер қадағалауға және дұрыс шешімдер қабылдауға негіз болатын үлкен деректерді талдайды. Автоматты қауіпсіздік шаралары: жасанды интеллект қауіпсіздік жүйелерін автоматтандыруға мүмкіндік береді. Мысалы, зиянды бағдарламаларды (вирус, троян) анықтау және олардың алдын алу автоматтандырылған жүйелер арқылы жүзеге асады. Фишинг және әлеуметтік инженерияға қарсы күрес: AI жүйелері фишингтік шабуылдарды анықтауға және пайдаланушылардың жалған сайттарға кіруін болдырмауға көмектеседі. Тәуекелдер: Жасанды интеллекттің өз бетінше басқарылуы: AI жүйелері шабуыл жасаушылар үшін жаңа мүмкіндік болуы мүмкін. Олар өздерінің алгоритмдерін айналып өту үшін интеллектуалды тәсілдерді пайдалана алады. Блокчейн технологиясы Блокчейн технологиясы ақпараттың қауіпсіздігін қамтамасыз етудің жаңа тәсілін ұсынады. Блокчейнде ақпарат блоктар түрінде сақталады, бұл технологияның негізгі ерекшелігі — деректердің өзгертілмейтіндігі. Бұл қасиет блокчейнді, әсіресе деректердің тұтастығын сақтауға бағытталған ақпараттық қауіпсіздік саласында тиімді етеді. Блокчейннің ақпараттық қауіпсіздікке әсері: Деректердің тұтастығы: блокчейн технологиясының бір ерекшелігі — деректерді өзгерту мүмкіндігінің болмауы. Бұл технология арқылы сақталған мәліметтер ешқашан өзгертілмейді, бұл оларды манипуляциядан қорғауға мүмкіндік береді. Дистрибутивті жүйелер: блокчейн мәліметтерді бірегей орыннан емес, бүкіл желі бойында таратады, бұл оның қауіпсіздігін күшейтеді. Тіпті жүйенің бір бөлігі бұзылса да, қалған бөлігі ақпаратты қорғап қалуы мүмкін. Аутентификация және сәйкестік: блокчейн технологиясы аутентификация процестерін жақсартуға мүмкіндік береді. Әрбір транзакция немесе әрекет блокчейнде тіркеледі, және оны тексеруге болады, бұл қауіпсіздікті арттырады. Тәуекелдер: Блокчейн жүйесінің масштабталуы: блокчейн жүйелерінің масштабталуы қазіргі

уақытта қиындық туғызады. Олардың жоғары деңгейдегі өнімділігі мен жылдамдығын қамтамасыз ету үшін жаңа шешімдер қажет. Желілік шабуылдар: блокчейннің қауіпсіздігін тексеру кезінде желілік шабуылдар (мысалы, 51%-дық шабуылдар) қауіп төндіруі мүмкін. Кванттық есептеу Кванттық есептеу — бұл қазіргі дәстүрлі компьютерлерден мүлдем жаңа тәсілмен жұмыс істейтін есептеу жүйелері. Кванттық есептеу қауіпсіздік саласына келетін болсақ, ол деректердің шифрлау әдістерін бұзудың жаңа жолдарын аша алады. Кванттық есептеудің ақпараттық қауіпсіздікке әсері: Шифрлау әдістерінің қауіпсіздігін бұзу: кванттық компьютерлер классикалық криптографиялық әдістерді (RSA, AES) жеңе алады. Кванттық есептеу алгоритмдері қазіргі шифрлау әдістерін бұзуды жеңілдетеді. Жаңа криптографиялық әдістер: кванттық есептеу жүйелерінің пайда болуы жаңа криптографиялық әдістерді дамыту қажеттілігін туғызады. Кванттық кілт алмасу сияқты жаңа әдістер ақпараттық қауіпсіздік саласында пайдаланыла бастайды. Тәуекелдер: Қазіргі шифрлау жүйелерінің осалдығы: кванттық есептеу дәуірі келген кезде қазіргі шифрлау әдістерінің жарамсыз болуы мүмкін, сондықтан жаңа тәсілдер мен шешімдер енгізу қажет болады.

Интернет заттары (IoT) және 5G технологиясы Интернет заттары (IoT) мен 5G желілері ақпараттық қауіпсіздікке үлкен әсер ететін тағы бір тренд болып табылады. IoT құрылғыларының санының артуы және 5G желісінің жоғары жылдамдығы қауіпсіздікке жаңа талаптар мен мәселелер туғызады. IoT және 5G технологияларының қауіпсіздікке әсері: Құрылғыларды қорғау: IoT құрылғыларының санының көбеюі және олардың байланысының қауіпсіздігі әрқашан тексеріліп отыруды талап етеді. Бұл құрылғылардың қауіпсіздігін қамтамасыз ету үшін жаңа шешімдер қажет. Жоғары жылдамдық пен кең таралған қосылымдар: 5G желілері арқылы деректерді көбірек және жылдам жіберу мүмкіндігі жаңа қауіптерді туғызады. Бұл деректердің ұрлануы немесе өзгертілуі қаупін арттырады. Тәуекелдер: IoT құрылғыларының осалдығы: IoT құрылғылары жиі қорғаусыз қалуы мүмкін, себебі олар өндірушілердің бастапқы күйінде әлсіз қауіпсіздік шараларымен жабдықталады.

ҚОРЫТЫНДЫ

Ақпараттық қауіпсіздік саласындағы болашақ трендтер ұйымдардың қауіптерді басқару, деректерді қорғау және қауіпсіздікті қамтамасыз ету тәсілдерін өзгертеді. Жасанды интеллект, блокчейн, кванттық есептеу, IoT және 5G сияқты жаңа технологиялар ақпараттық қауіпсіздікке жаңа мүмкіндіктер мен тәуекелдер әкеледі. Бұл технологиялар ақпараттық жүйелерді қорғау саласында тиімді шешімдер ұсына отырып, жаңа қауіптерді де туындатуы мүмкін.

Бақылау сұрақтары: 1.Жасанды интеллект пен машиналық оқыту ақпараттық қауіпсіздік саласына қалай әсер етеді? 2.Блокчейн технологиясының ақпараттық қауіпсіздікке әсері қандай? 3.Кванттық есептеу технологиясы шифрлау әдістерін қалай бұза алады? 4.Интернет заттары мен 5G технологияларының ақпараттық қауіпсіздікке ықпалы қандай? 5.Ақпараттық қауіпсіздік саласында болашақта пайда болуы мүмкін жаңа қауіптер мен мүмкіндіктерді сипаттаңыз.