Министерство образования и науки Республики Казахстан

Евразийский национальный университет им. Л.Н.Гумилева

Институт информационной безопасности и криптологии

СБОРНИК ТРУДОВ

III Международной научно-практической конференции

«Информационная безопасность в свете Стратегии Казахстан - 2050»

15-16 октября 2015 года, г. Астана

УДК 004 (063)

ББК 32.973

С23

Рецензенты:

1. Е.Н. Сейткулов, к.ф.-м.н., директор института информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева
2. Н.Н.Ташатов, к.ф.-м.н., заведующий лабораторией кодирования и защиты информации информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева

С23 Сборник трудов III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан-2050», 2015. – 400 стр.

ISBN 978-9965-31-722-4

Сборник подготовлен по материалам III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан - 2050». Тематика сборника охватывает такие вопросы, как проблемы обеспечения информационной безопасности в государственных и бизнес структурах, информационная безопасность компьютерных систем, математические проблемы защиты информации. Представлены результаты научных исследований, проведенных в вузах и научно-исследовательских организациях Казахстана, России, Белоруссии и др.

УДК 004 (063)

ББК 32.973

Утверждено и рекомендовано к изданию научно-техническим советом института информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева. Протокол № 2 от 19 сентября 2015 года.

ISBN 978-9965-31-722-4

/ дешифрования AES можно соответственно заменить на композиции $AES(F_k^{d_e}(S))$ / $F_k^{d_e}{}^{-1}(AES^{-1}(S))$.

Литература

1. Odlyzko A. M. and Lagarias J. C. Solving Low-Density Subset Sum Problems // J. Association Computing Machinery. 1985. V. 32. No.1. P. 229–246.

2. Александров А.В., Метлинов А.Д. «К вопросу об особенностях реализации симметричной рюкзачной криптосистемы с общей памятью и плотностью укладки больше единицы» // XXXIII Всероссийская НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем», г. Серпухов, сборник научных трудов, часть 4, с. 161-167, 2014.

3. Александров А.В., Метлинов А.Д. Симметричная рюкзачная криптосистема с общей памятью и плотностью укладки больше единицы // Журнал «Проблемы информационной безопасности. Компьютерные системы», №4 2014, с. 58-65.

Мусиралиева Ш.Ж., Абдаким Г.

ЗАМАНАУИ ТЕХНИКАЛЫҚ ҚАУІПСІЗДІК ЖҮЙЕЛЕРІ ҮШІН ПРОЕКТІЛІК ШЕШІМДЕР

әл-Фараби атындағы ҚазҰУ, Алматы

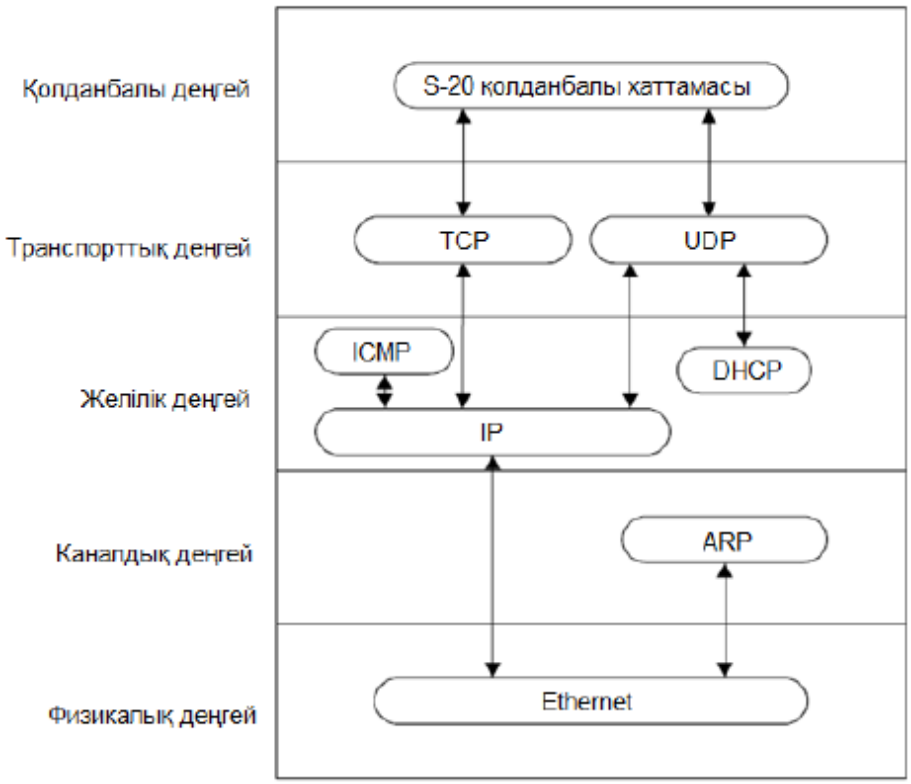
Қазіргі кезде кез келген кәсіпорынның тіршілік әрекетін қауіпсіздіктің енгізілген жүйесінсіз елестету қиын. Егер бұрын талап периметрдің қорғанысымен шектелсе және бейне бақылау ғана болса, ал бүгін қауіпсіздіктің техникалық жүйесі басқа да көптеген міндеттерді шешеді. Кәсіпорынның басқарылуының қамтамасыз етілуі, объектілерді қорғау, еңбектиімділігінің жоғарылауы, экономикалық тиімділік көптеген мәселелердің бірі болып табылады, олардың шешу жолдарын қазіргі қауіпсіздіктің жүйелерінің мүмкіндіктерімен толықтыруға болады. Осылайша, жүйе өзін-өзі қорғаныс

құралдары мен инженерлік-техникалық құралдардан тұратын интегралданған кешен ретінде таныстыруы керек; ұйымдастыру шаралары; ақпарат қорғауды жүзеге асыру міндеттерін қажетті хаттамамен бағдарламалық қамтамасыз ету; жиынның бағдарламалық қаражаты және деректерді визуализациялау және тағы басқа ([1,2]).

Ұсынылып отырған баяндамада авторлар *PERCo-S-20* техникалық қауіпсіздік жүйесіне сүйене отырып жоғары оқу орындары үшін проектілік шешімдер ұсынып отыр.

Желілік бақылауыштардың қызмет етуі үшін Ethernet 10-BaseT, 100-BaseTX немесе 1000-BaseTX желі қажет. Деректерді жіберу үшін бақылауыштардың тікелей IP-адрестерін, сонымен бірге UDP хаттаманы пайдаланады. *PERCo-S-20* жүйесін қолданатын объектілердегі деректерді жіберуді дұрыс күйге келтіру үшін дайын жүзеге асырылған механизмді түсіну қажет. ([3]). Жүйеде деректер алмасу үшін келесі хаттамалар тобы қолданылады (1-сурет):

Бірлестірілген хаттамалар бойынша функционалды қызмет жасайтын, ортақ байланыс сызықтары мен мәліметтер қорын қолданатын, ортақ программалық ядро арқылы басқарылатын, барлық кішігірім жүйелердің бір үлкен комплексті жүйеге біріктіру техникалық қауіпсіздік жүйесін құрудың қазіргі заманғы көзқарасы болып табылады. Бірақ қауіпсіздік жүйені толығымен автоматтандырылған түрде жасауға болмайды. Өйткені ұйымда дәл қазіргі уақытта болып жатқан және болашақта болуы мүмкін барлық жағдайларды қарастыру мүмкін емес. Моделдеуді құрал-жабдықтардың көмегімен жасау мүмкіндігін қолдана отырып осы мақаланың авторлары еңбектің тиімділігін жоғарылату үшін Ақпараттық жүйелер кафедрасына арналған проектілік жоба жасады және тест жүргізді.



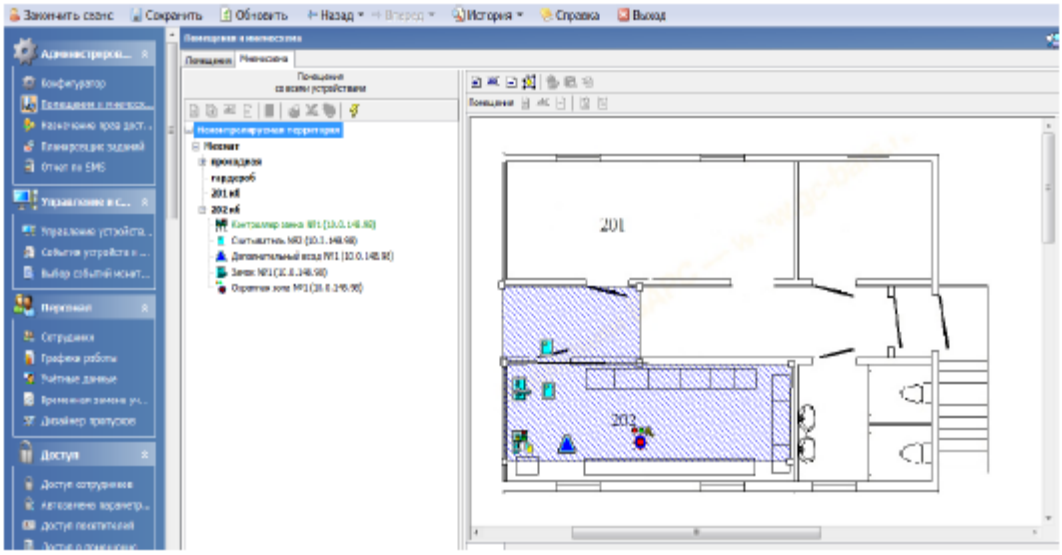
1-сурет. Деректер алмасуға арналған хаттамалар

Бастапқы кезеңде қауіпсіздік жүйесінің сырт пішіні жасалады. Бұл кезең *PERCo-S-20* қауіпсіздік жүйесінің программалық қамтамасыз ету және құрылғылардың параметрлерінің жұмыс істеуін сипаттауға арналған. Бұл кезде жүйеге жаңа құрылғыларды қосу немесе құрылғыларды алып тастау, құрылғылардың жұмысын қалыпқа келтіру, әр түрлі оқиғаға байланысты құрылғылардың реакциясын бақылау сияқты жұмыстар атқарылады.

Моделдеу сатысы КІТ оңтайлы зертханалық стендінде жүзеге асырылды. КІТ жиынтығы PERCo-CT/L-04 контроллерінен және екі PERCo-IR0X сериясындағы есептегіштен, өткізгіш құрылғыдан тұрады.

Қызметкерлердің мәліметтер қоры жасалды, жұмыс кестесі құрылды, кіруге мүмкіндік беретін карточкалар берілді және кіруге шек қою жасалды. Мынадай жағдайларда: мұғалімнің сабаққа 10 минуттан көп кешігуіне

байланысты немесе мұғалімнің аудиторияда сабақтың соңына дейін болмауы кезінде тәртіп бұзу туралы журнал құрылады. Механика-математикалық факультеттің екінші қабатының сол жақ қанатының мнемосхемасы жасалды. 2-суретте көрсетілгендей 202-аудиторияда контроллер, 2 есептегіштер, құлып орналасқан. Бұл кезеңде жасалған жұмыстар келесі кезең үшін де пайдаланды.



2-сурет. Құрылғылар қойылған мнемосхема

СМС жолдауды баптау. Бұл кезеңде механика-математикалық факультеттің ақпаратық жүйелер кафедрасының мәліметтер қорындағы белгілі бір оқиғалар орын алған жағдайда жұмыс өнімділігін жоғарылату мақсатында берілген номерге СМС жолдау мүмкіндігі қарастырылды.

GSM модемді қолдана отырып SMS-тараттуларды (рассылка) орнату. Алғашқыда модем ретінде, USB порт арқылы компьютерге қосыла алатын және де ішкі модеммен жабдықталған ұялы телефон қолданылды. Мұндай ұялы телефон, аз мөлшердегі SMS таратуға жарамды, ал көп мөлшердегі SMS-таратуларды жіберу үшін USB-модем қолданылмақ.

SMS-провайдер арқылы смс-тараттуларды орнату. Іске асыру барысында QuickTelecom(http://sms1.quicktelecom.kz) компаниясы смс провайдер ретінде

таңдалды. Мұндай программалық модульді орнату барсында SMPP протоколы қолданылады.«SMS» (Short Message Service, қазақша транскрипциясы: «СМС») - бұл байланыстың жылжымалы және жердегі желілері, соның ішінде GSM стандартының ұялы телефондары үшін арналған қысқа мәтінді хабарламалар, олардың мәтіндері әріптерден, сандардан және басқа белгілерден тұруы мүмкін; SMS – хабарлама екі түрлі форматта жасалуы мүмкін: Unicode (соның ішінде орыс тілі) және 7bit (ағылшынша мәтін және көп көлемдегі символдар). Хабарлама бір немесе бірнеше SMS-тен тұруы мүмкін. Бір хабарламадағы SMS санын енгізілген мәтін негізінде есептеу unicode формуласы бойынша жүргізіледі: егер ұзындығы <=70, онда 1 SMS, басқаша, SMS саны былай анықталады: SMS саны = символдық хабарламаның ұзындығы/67 (мысалы, 135 символдан тұратын ұзындықтағы мәтін 3 SMS хабарлама ретінде саналады). 7bit: егер ұзындығы <=160, онда 1 SMS, басқаша, SMS саны былай анықталады: SMS саны = символдық хабарламаның ұзындығы/ 153 (мысалы, 310 символдан тұратын ұзындықтағы мәтін 3 SMS хабарлама ретінде саналады).

Аудиторялық қорды визуализациялау. Белгілі-бір іс-шараларды өткізуге аудиторияларды іздеу немесе сабақ кестесі өзгерген кезде мұғалімдер факультет диспетчерлеріне хабарласады. Аудиторияларды іздеу көп уақыт алмайды. Ұсынылып отырған программалық жабдықтама біздің факультет диспетчерлеріне көмек ретінде жасалынып отыр. Сонымен қатар техникалық қауіпсіздігі бар кез келген мекемеде қолданса болады. Сабақтың реттік нөмірін және аудиторияның түрін таңдағанда, нәтижесі экранға шығады. Курсорды сабақ батырмасына апарған кезде, аудитория түрі мен аудиторияның сыйымдылығын көрсетеді. Экранда белгілі бір уақыт кезіндегі аудиторияның бос болмауы қызыл түспен көрсетілінеді. Ізделінді уақыт кезінде аудиторияның бос болып, бірақ сыйымдылығы сәйкес келмейтін аудитория сұр түспен көрсетілінеді. Программада лекция өтуге арналған аудитория 25-тен асатын сыйымдылықпен, ал семинар сабақтарға 25-тен кем сыйымдылықпен жасалынған. Сонымен қатар программада, зертханалық аудиторияда семинар

немесе лекция сабақтарын өтуге болмайтынын да көруге болады. Визуализациялау программасы C# тілінде жазылды. Жұмыстың нәтижесін http://www.studenthelp.kz сайтынан таба аласыз.

Қолданылған әдебиеттер

1. ХоффманЛ.Дж. Современные методы защиты информации. М.: Сов. Радио, 1980 г.
2. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2001 – 496 с
3. Единая система S-20. Руководство администратора. Доступно на http://www.perco.ru
4. Мусиралиева Ш.Ж, Бекбулатов Е. О курсе «Технические системы безопасности», Труды международной конференции "Применение информационно-коммуникационных технологий в образовании и науке" , Алматы, 22-23 ноября 2013 года.

Нурланова Б.М., Жумагулова С.К., Алибиев Д.Б.

АҚПАРАТТЫ ҚОРҒАУДЫҢ КРИПТОГРАФИЯЛЫҚ ӘДІСТЕРІН ҚОЛДАНУДЫҢ КЕЙБІР АСПЕКТІЛЕРІ

Академик Е.А.Бөкетов атындағы Қарағанды мемлекеттік университеті
Қарағанды қаласы, Қазақстан Республикасы

Қазақстан Республикасының Еуразиялық аймаққа кіруі, XXI ғасырға аяқ басуы ел Президентінің «Қазақстан-2030» атты стратегиялық бағдарламасына сәйкес жаңа техника мен технология үдерістерінің дамуы, келешекте жоғары оқу орындарында білім беру қандай бағытта өрбуі керек деген өзекті мәселе туғызады. Барлық өркениетті елдерде азаматтардың қауіпсіздік сақшысы ретінде заңдар тұр, барлық есептеуіш техника саласында құқық қолданатын іс-тәжірибе әзірге дамымаған, ал заң шығарушы процесс технология дамуына