Закирова Одина Гулямовна
Ўзбекистон Республикаси Ички Ишлар вазирлиги Академияси Ҳуқуқбузарликлар профилактикаси ва криминология кафедраси, ю.ф.д. профессор
Нурбобоева Фарангиз Бурхон қизи
Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Ҳуқуқий сиёсат тадқиқот институти, етакчи маслаҳатчи

АХБОРОТ ВОСИТАЛАРИДАН ФОЙДАЛАНГАН ҲОЛДА СОДИР ЭТИЛАЁТГАН ЖИНОЯТЛАР ХАВФИНИ СУҒУРТАЛАШ ЗАРУРИЯТИ

Закирова Одина Гулямовна
Профессор, доктор юридических наук кафедры Профилактики правонарушений и криминологии, Академия Министерства внутренних дел Республики Узбекистан,
Нурбобоева Фарангиз Бурхон кизи
Ведущий консультант, Исследовательский институт правовой политики при Министерстве юстиции Республики Узбекистан

НЕОБХОДИМОСТЬ СТРАХОВАНИЯ РИСКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Zakirova Odina
Academy of the Ministry of internal affairs of the Republic of Uzbekistan, Department of offenses profilactics and criminology, Doctor of Law., professor
Nurboboeva Farangiz
The Research Institute of Legal Policy under The Ministry of Justice, Leading consultant

THE NEED TO INSURANCE THE RISK OF CRIME COMMITTED WITH THE USE OF INFORMATION TECHNOLOGIES

Аннотация. *Ушбу мақолада бугунги кундаги долзарб масалалардан бири бўлган ахборот рискларини суғурталаш мавзусига тўхталиб ўтилади. Ушбу суғурта турининг ўзига хос характерли хусусиятлари, кибержиноятлар билан узвий боғлиқлиги ва бугунги кундаги долзарблиги масалалари таҳлил қилинади. Мақоланинг мақсади ҳар қандай компаниянинг иш фаолиятида муҳим аҳамиятга эга бўлган маълумотларнинг, маблағларнинг ўғирланишидан ва уларга зарар етказлишидан ҳимоя қилишга қаратилган киберсуғуртанинг мазмун-моҳияти ва зарурияти очиб беришдан иборат.*

Калит сўзлар: *кибержиноятлар, киберсуғурта, ахборот хавфлари, ахборот хавфсизлиги, киберҳужум, киберхавф.*

Аннотация. *В данной статье основное внимание уделяется страхованию информационных рисков, которое на сегодняшний день является одним из наиболее актуальных вопросов. Будут проанализированы особенности данного вида страхования, его неотъемлемая связь с киберпреступностью, актуальность на сегодняшний день. Цель статьи – раскрыть сущность и необходимость содержания киберстрахования, которое направлено на защиту информации, средств, имеющих важное значение в деятельности любой компании, от кражи и ущерба.*

Ключевые слова: *киберпреступность, киберстрахование, информационные угрозы, информационная безопасность, кибератака, киберугроза.*

Abstract. *This article focuses on information risk insurance, which is one of the most pressing issues today. The specific features of this type of insurance, its integral connection with cybercrime, and its relevance today will be analyzed. The purpose of the article is to reveal the essence and necessity of the content of cyber insurance, aimed at protecting against theft and damage to information, funds, which are important in the activities of any company.*

Key words: *cybercrime, cyber insurance, information threats, information security, cyber-attack, cyber-threat.*

Ривожланиб бораётган замонавий жамиятнинг асосий белгиси, аввалambор, бугунги кунда ахборотлаштиришнинг рақамли тусда шаклланишида намоён бўлмоқда. Дунёнинг кўплаб мамлакатларида ахборот технологияларининг ривожланиши, ўз навбатида, бу соҳада янги турдаги жиноятларнинг содир бўлишига ҳам шароит яратиб бермоқда. Шундай жиноятлардан бири бу жиноят ҳуқуқи учун янги турдаги атама ҳисобланувчи кибержиноятларнинг кўплаб учрашидир.

Таъкидлаш жоизки, рақамли технологиялар соҳасидаги жиноятлар ҳақида сўз кетганда, кибержиноятлар тушунчасининг ўзи нимани англатиши борасида савол пайдо бўлиши ҳам турган гап. Бу борада олимлар турли қарашларга эга бўлган ҳолда “кибержиноят” ва “компьютер жиноятлари” атамаларининг бир-бирига ўхшаш ва фарқли жиҳатларига оид фикрлар билдиришган. Шунга кўра, кибержиноят – бу компьютер тизимлари ёки компьютер тармоқлари, шунингдек, кибермаконга киришнинг бошқа усуллари ёрдамида ёки улар орқали кибермакондан компьютер тизимлари ёки тармоқлари воситалари доирасида ҳамда компьютер тизимларига, компьютер тармоқларига қарши содир этилган ҳар қандай жиноятлар мажмуидир [1].

Ахборот воситаларидан фойдаланган ҳолда содир этилаётган жиноятлар сонининг ортиб бориши бу каби жиноятлар натижасида етказилиши мумкин бўлган зарарларнинг олдини олиш мақсадида кибержиноятлардан ҳимояланиш воситаларини излашни тақозо этади. Шундай ҳимоя усулларидан бири киберхавфларни суғурталаш бўлиб, рақамли хавфларни суғурталаш киберҳужумлар ва уларнинг салбий оқибатларидан ҳимояланишнинг мақбул кўринишларидан биридир. Киберсуғурта – ҳар қандай компания ишининг бевосита ёки билвосита равишда маълумотларни сақлаш ва қайта ишлаш билан боғлиқ бўлган суғурта фаолиятини ўз ичига олади [2. Б. 13].

Бошқачароқ қилиб айтганда, киберсуғурта – юридик ва жисмоний шахсларнинг интернетдан фойдаланиши, хавфсизлик тизимининг бошқалар томонидан бузиб кирилиши орқали электрон шаклда сақланган маълумотларни, ахборот технологиялари инфратузилмасининг муҳим манбаларини, ҳисоб рақамлардан нақдсиз пул маблағларининг ўғирланиши билан боғлиқ хавфлардан ҳимоя қилиш учун мўлжалланган суғурта маҳсулотидир. Бугунги кунда нақд пул маблағларидан кўра нақдсиз пул маблағларини ўғирлаш нисбатан осонроқ бўлганлиги, ҳимоя кодларини бузиб киришда хакерлар томонидан бинолар деворини бузишга нисбатан камроқ қийинчиликка учраётганликлари айнан кибержиноятларнинг ва унинг натижасидаги хавфларнинг ортишига сабаб бўлмоқда.

Айтиш лозимки, ҳозирда бошқа турдаги жиноятлар қаторида кибержиноятлар дунёда кенг тарқалган долзарб муаммоли ҳодисага айланиб улгурмоқда. Молиявий хизматлар соҳасидаги жиноятларнинг умумий ҳажмида унинг улуши тахминан 40% ни ташкил этиб, қамраб олиши бўйича даромадларни ноқонуний ўзлаштиришдан кейинги ўринда туради [3. Б. 45]. Дунё бўйлаб йирик хакерлик ҳужумларининг содир бўлиши киберсуғуртага зарурият борлигини кўрсатмоқда. Мисол тариқасида, 2014 йилда **Америкининг** “Yahoo” (дунёда иккинчи ўриндаги энг машҳур қидирув тизими) компанияси серверларига амалга оширилган ҳужумдан сўнг биргина Америкининг ўзида киберрисклар суғурталанишига бўлган талаб 3 баробарга ортди [4]. Ушбу вазиятда хакерлар томонидан тахминан 500 млн. фойдаланувчиларнинг аккаунтлари бузилиши натижасида уларга абонентларнинг туғилган кун саналари, телефон рақамлари ва пароллари каби шахсий маълумотлар маълум бўлган. Шунингдек, **Россияда,** 13 мингдан ортиқ компьютерлар “Wannacry ва Petya” бузғунчи хакерлари таъсирига учраганидан сўнг бундай суғуртага бўлган талаб 30 фоизга ортган. Улар томонидан абонентлар маълумотларини блокдан чиқариш учун 300 доллардан 600 долларгача бўлган маблағ талаб этилиб, тўловни биткоинларда амалга оширилиши сўралган [5].

Шунингдек, **Даниянинг** йирик саноат компанияси “Moller-Maersk”ни ҳам киберҳужумлар четлаб ўтмаган. Ушбу компания ҳам киберхавфлардан ҳимояланмаганлиги сабабли 200 млн. доллардан ортиқ зарар кўрган. Бундай ҳужумлардан сўнг “AIG” суғурта компаниясида мижозларнинг ахборот хавфларини суғурталаш бўйича сўровлари 38%га кўпайган [6. Б. 47].

Ахборот воситаларидан фойдаланган ҳолдаги ҳуқуқбузарликларнинг сони ортиб бораётган экан, кибержиноят хавфи остида қолаётган соҳалар, биринчи навбатда, банклар, инвестиция компаниялари, қимматли қоғозлар бозори иштирокчилари, электрон тўловлар тизими, суғурта компанияларининг ўзлари ва, шунингдек, кичик, ўрта ва катта бизнес субъектлари ҳисобланади. Бошқа компаниялар ҳам “nou-xau”, инновация янгиликлари, ходимларнинг шахсий маълумотлари, муҳим бизнес янгиликлари каби қимматли маълумотларнинг ўғирланиши хавфи остида бўлишлари мумкин. Таҳлиллар шуни кўрсатадики, кибержиноятларнинг асосий зарари молиявий ва моддий кўринишга эга бўлади.

Киберҳужумларнинг кўплаб содир бўлаётганлиги эвазига бу каби ҳужумларнинг оқибатларини суғурталаб қўйиш амалиёти ҳам бир мунча давлатларда йўлга қўйилган. Бундай давлатларга мисол тариқасида Украина, Қозоғистон, Германия, Буюк Британия, АҚШ давлатларини келтириш мумкин. Бугунги кунда дунёдаги энг йирик суғурта компаниялари сифатида “American International Group” (AIG), “Allianz Group”, “Berkshire Hathaway”, “Lockton Companies”, “Chubb Limited”, “Munich Re Group”, “AXAXLSA”, “Zurich Insurance Group” ва “Lloyd’s Group of London Ltd”ларни санаб ўтиш мумкин.

Жаҳон амалиётида суғурта компаниялари томонидан қуйидаги хавф турлари бўйича суғурта турлари таклиф этилмоқда:

- махфий маълумотларни ўғирлаш ва ундан ташкилот ходимлари томонидан кейинчалик фойдаланиш хавфи;
- жиноятчилар томонидан банк мижозлари ҳақидаги маълумотларни, масалан, кредит карта ва ҳисоб рақамларига оид ахборотларни ўғирлаш хавфи;
- банк мижозларининг ҳисоб варақларидан ноқонуний рухсатсиз пул ечиб олиш хавфи;
- компания ходимларининг махфий маълумотларни ошкор қилиш хавфи;
- компьютер тармоғидаги, ташкилотнинг веб-сайтидаги носозликлар туфайли корхона фаолиятининг номаълум муддатга тўхтатилиши хавфи;
- ташкилот томонидан нотўғри маълумотларнинг жойлаштирилиши эвазига зарар кўриш ва ҳоказолар [7. С. 15].

Суғурта компаниялари томонидан кибержиноятларнинг суғурта қилинишининг таклиф этилиши кибержиноятлар оқибатида зарар кўрган компаниялар учун катта йўқотишларнинг олдини олиш, корхоналарнинг нормал фаолият йўналишига қайтишига, барқарорликни сақлашга, тўлов қобилияти ва ҳар хил турдаги кибертаҳдидлар туфайли ишлаб чиқаришдаги узилишлар натижасида йўқотишларни камайтириш ҳамда молиявий механизмларни таъминлашга ёрдам беради.

Шунингдек, суғурта компаниялари томонидан киберхавфларнинг суғурталаниши ва унда суғурта пулларининг тўлаб берилишида қуйидагилар: жумладан, киберхавфлар бўйича маълумотларни йиғиш, инфратузилма заифлигини сканерлаш, киберхавфларни таҳлил қилиш, киберхавфсизлик тизимларининг бардошлилигини баҳолаш, киберхавфсизлик масалалари бўйича маслаҳатлар бериш, ўқитиш ишларини олиб бориш, киберхавфсизлик инфратузилмасини стресс тестлаш ҳам инобатга олинади.

Шуни ҳам алоҳида айтиб ўтиш лозимки, йирик суғурта компанияларининг аксариятида бир нечта суғурта ҳодисаларини суғурталашни назарда тутувчи суғурта пакетлари таклиф этилиши ҳам мумкин. Хусусан, “American International Group”нинг “CyberEdge” суғурта дастури доирасида қуйидаги зарарлар қопланиши мумкин:

1) суғурталанган шахснинг тармоқ хавфсизлиги ёки махфий маълумотларнинг ҳимояланмаганлиги натижасида келиб чиқадиган ёки молиявий йўқотишларни даъво қиладиган учинчи шахсларнинг даъволари бўйича зарарлар;

2) суғурталанган шахснинг тармоқ хавфсизлигининг бузилиши ёки махфий маълумотларнинг ҳимояланмаганлиги натижасида келиб чиқадиган тартибга солувчи ҳаракатларни текшириш ва ҳимоя қилиш, шу жумладан, қонун ҳужжатларида рухсат этилган ҳолларда бундай жарималарни қоплаш;

3) киберҳодисаларни бошқариш ва оқибатларини енгиллаштиришга ёрдам бериш учун хабарлар, жамоатчилик билан алоқалар ва бошқа хизматларнинг харажатлари;

4) қопланган киберҳодисани тугатиш учун тўловларни амалга ошириш;

5) икки нусхадаги электрон маълумотларни қайта тиклаш харажатлари ёки имкони бўлмаса, қопланадиган киберҳодиса туфайли электрон маълумотларни ўрганиш, тўплаш ва йиғиш харажатлари ва бошқалар.

Суғурта компаниялари томонидан кибержиноятлар натижасида етказилган зарарнинг қопланиши ва суғурта мукофотининг тақдим этилиши жараёни қуйидаги босқичларни қамраб олади. Жумладан, биринчи босқичда ахборот воситаларидан фойдаланган ҳолда кибержиноят воқеаси юзага келади, кейинги босқичда ушбу воқеа юзасидан суғурта ташкилотига хабар берилади, учинчи босқичда ушбу воқеа юзасидан суғурта ташкилотининг муносабат билдириши амалга оширилади, тўртинчи босқичда, суғурта ташкилоти томонидан ҳужумга учраган компанияга оид ҳужжатларни йиғиш ва таҳлил қилиш ишлари амалга оширилиб, етказилган зарарнинг ўзига хослиги жиҳатлари суғурта компанияси томонидан баҳоланади. Ҳужжатлар таҳлили ва баҳолаш натижасига кўра, суғурта компаниясининг суғурта зарарини қоплаш ишлари амалга оширилади.

Мамлакатимизда ҳам бошқа давлатларда бўлгани сингари кибержиноятлар, ҳисоб рақамларидан пул маблағларининг ечиб олиниши, шахсга доир бўлган ва махфий аҳамиятга эга бўлган маълумотлар базаларининг бузиб кирилиши ва ўғирланиши ҳолатлари бўйича жиноятлар учраб турибди. Кибежиноятларга қарши курашиш ва унга қарши туришда юзага келиши мумкин бўлган киберхавфларнинг олдини олишда давлатимизда киберрискларнинг суғуртланиши амалиёти ва механизмининг ҳали ривожланмаганлиги ва мавжуд эмаслиги ушбу соҳадаги асосий муаммолардан бири саналади. Бундан ташқари, республикада фаолият кўрсатувчи суғурта компаниялари учун ҳам бундай турдаги суғурта тарифлари янги тушунча ҳисобланиб, уларнинг бу борада тажрибаси етарли эмас. Бу эса, ўз навбатида, барча тадбиркорлик субъектлари, молиявий бирлашмалар, банклар фаолияти ва улардаги маълумотлар базаларининг хавф ортида қолаётганлигидан далолат беради.

Шубҳасиз айтиш мумкинки, киберсуғурта киберҳужумларнинг содир бўлишидан олдин ҳам мижозларнинг маълумотларини ҳимоя қилишда ёрдам бериши мумкин. Яъни суғурта дастурлари ўз ичига аудит хизматларини таклиф этган ҳолда унда экспертлар томонидан мижозларнинг энг муҳим рисклари кўрсатиб берилади ва уларни минималлаштириш бўйича тавсиялар ҳам тақдим этилади. Киберсуғуртанинг суғурта бозорини қамраб олиш потенциали бошқа турдагиларга қараганда анча юқори бўлиб, бу киберхавфларнинг нафақат маълумотлар базалари, банк маълумотлари билан балки турли тадбиркорлик субъектлари, ижтимоий тармоқлардаги шахсий профиллар, электрон почталар, онлайн ўйин компаниялари ва давлат органларининг фаолияти билан ҳам узвий боғлиқлигида кўринади. Киберсуғурта бозорини ривожлантириш учун харажатларни камайтириш ва минималлаштириш, рақобатдош устунликларга эга бўлиш учун рақамли узатиш ва виртуал хизматни кенгайтириш лозим.

Халқаро давлатлар тажрибасига биноан, шунингдек, юртимизда ҳам кибержиноятларнинг ортиб бораётганлигининг олдини олиш борасида бир қадам олдинга силжиш мақсадида Ўзбекистон Республикасида киберхавфсизликни суғурталаш амалиётини яратиш ва такомиллаштириш бўйича қуйидаги таклифлар илгари сурилади:

1) Ўзбекистон Республикасида ахборот хавфсизлигининг асосий таҳдидларини суғурталаш мақсадида юридик ва жисмоний шахслар учун киберсуғуртани жорий этиш;

2) киберхавфсизликни таъминлаши лозим бўлган ваколатли давлат органларининг асосий фаолият йўналишларини белгилаш;

3) киберхавфсизликни суғурта қилишнинг асосий методологияси, киберхавфларни баҳолашнинг асосий тавсиявий шартларини белгилаш;

4) киберсуғурта фаолиятини амалга ошириш мақсадида ривожланган хорижий мамлакатларнинг бу борадаги тажрибасини чуқур ўзлаштириш ва амалиётга жорий этиш;

5) киберсуғурта фаолиятини амалга оширувчи ходимларнинг ушбу соҳада малакасини ошириш.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/ kiberprestupnost-kak-novayakriminalnaya-ugroza (дата обращения: 15.04.2020).

2. Иванов И.К. Кибер-страхование: как обеспечить информационную безопасность бизнесу // Большой портал для малого бизнеса – 2016, – №16, С. 13–24

3. Мамаева Л.Н. Ларионов В.И. Кибер-страхование как способ обеспечения информационной безопасности // Экономическая безопасность и качество – 2018. – №1 (30). С. 76–79.

4. Волкова Т.А. Суслякова О.Н. Страхование информационных рисков (киберстрахование) // Инновационная экономика: перспективы развития и совершенствования – 2018 №7 (33), Том 1. – С. 117.

5. Волкова Т.А. Суслякова О.Н. Страхование информационных рисков (киберстрахование) // Инновационная экономика: перспективы развития и совершенствования – 2018 №7 (33), Том 1. – С. 117.

6. Номоконов В.А. Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра – 2017. –
№ 24. – С. 45–55.

7.Романенко Н.А. Страхование информационных рисков предприятий как инструмент риск-менеджмента // Финансовые исследования – 2018. – №7. – С. 13–24.