Кибер халдлага зөрчилтэй тэмцэх нийтийн төв УТҮГ-ын
захирлын 2024 оны ... дугаар сарын ....-ны.... өдрийн
... дугаар тушаалын ... хавсралт

СУРГАЛТЫН ХӨТӨЛБӨР

Нэр	Мэдээллийн аюулгүй байдлын чиглэлээр мэргэшүүлэх сургалт
Зорилго	Байгууллагын мэдээллийн аюулгүй байдал хариуцсан албан хаагчдад МУ-ын кибер аюулгүй байдлын тогтолцоо, хууль эрхзүй, зохицуулалтын орчны талаарх мэдлэг олгох, ISO27001-д суурилсан мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (МАБМТ)-г бий болгох, хэрэгжүүлэх, удирдах, хадгалах чиглэлээр иж бүрэн ойлголт өгөх, кибер халдлага, зөрчлийн үед хариу арга хэмжээ авах чадварыг эзэмшүүлэх замаар байгууллагуудын мэдээллийн аюулгүй байдал хариуцсан хүний нөөцийг чадавхжуулах зорилготой.
Оролцогчид	Байгууллагын мэдээллийн аюулгүй байдал хариуцсан албан хаагчид
Холбогдох бичиг баримт	Мэдээллийн аюулгүй байдлын чиглэлээр мэргэшүүлэх сургалтын хөтөлбөр
Зорилтууд	• Байгууллагын мэдээллийн аюулгүй байдал хариуцсан албан хаагчдад МУ-ын кибер аюулгүй байдлын тогтолцоо, хууль эрхзүй, зохицуулалтын орчны талаарх мэдлэг олгох; • ISO27001-д суурилсан мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (МАБМТ)-г бий болгох, хэрэгжүүлэх, удирдах, хадгалах чиглэлээр иж бүрэн ойлголт өгөх; • Кибер халдлага, зөрчлийн үед хариу арга хэмжээ авах чадварыг эзэмшүүлэх;
Урьдчилсан шаардлага	Мэдээлэл, харилцаа холбооны чиглэлээр бакалаврын зэрэгтэй. Кибер аюулгүй байдлын анхан шатны мэдлэгтэй байх.
Сургалтын агуулга (8 цаг лекц, 16 цаг дадлага ажил, нийт 24 цаг)	
	Модуль 1. Хууль эрх зүй, зохицуулалтын орчин
	Хичээл 1 (2ц) 2.1. Монгол улсын кибер аюулгүй байдлын тогтолцоо 2.2. Дасгал ажил болон хэлэлцүүлэг **Хичээл 2:** (2ц) 2.3. Кибер аюулгүй байдлын тухай хууль 2.4. Кибер аюулгүй байдлын тухай хуулийн дагалдах журмууд

Сургалтын агуулга 12 хичээл (1 хичээл = 90 min)	2.5. Дасгал ажил болон хэлэлцүүлэг **Хичээл 3:** (2ц) 3.1. Мэдээллийн аюулгүй байдлын бодлого боловсруулах үйл явц 3.2. Мэдээллийн аюулгүй байдлын бодлогын баримт бичгүүд, хэрэгжүүлэх арга замууд 3.3. Зарим улс оронд хэрэгжүүлдэг мэдээллийн аюулгүй байдлыг хангах стандартууд болон фрэймворкуудын тухай 3.4. Дасгал ажил болон хэлэлцүүлэг **Хичээл 4:** (2ц) 4.1. Мэдээллийн аюулгүй байдлын олон улсын эрх зүйн тогтолцооны тухай 4.2. Кибер гэмт хэргийн эрх зүйн зохицуулалтын орчин 4.3. Дасгал ажил болон хэлэлцүүлэг
	Модуль 2. Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо (ISO27001:2022)
	Хичээл 5: (2ц) 5.1. Хамрах хүрээ, эшлэл, нэр томьёо тодорхойлолт / ISO27001 стандартын 1-3 бүлэг / 5.2. Байгууллагын төлөв байдал /ISO27001 стандартын 4-р бүлэг/ 5.3. Манлайлал Манлайлал ба үүрэг амлалт, Байгууллагын үүрэг хариуцлага, эрх мэдэл /ISO27001 стандартын 5-р бүлэг/ **Хичээл 6:** (2ц) 6.1. Төлөвлөлт Эрсдэл боломжид чиглэсэн арга хэмжээ Эрсдэлийг бууруулах арга, МАБ-ын зорилтод хүрэх төлөвлөгөө /ISO27001 стандартын 6-р бүлэг/ 6.2 Дэмжлэг МАБ-ын шаардлагатай нөөц, мэдлэг, харилцаа холбоо, чадавх, баримтжуулсан мэдээлэл /ISO27001 стандартын 7-р бүлэг/ 6.3. Дасгал ажил болон хэлэлцүүлэг **Хичээл 7:** (2ц) 7.1. Ажиллагаа Төлөвлөлт ба хяналт, МАБ-ын эрсдэлийн үнэлгээ /ISO27001 стандартын 8-р бүлэг/ 7.2 Гүйцэтгэлийн үнэлгээ Хяналт, хэмжилт, дүн шинжилгээ, үнэлгээ, дотоод аудит, УДШ /ISO27001 стандартын 9-р бүлэг/ 7.3 Дасгал ажил болон хэлэлцүүлэг **Хичээл 8:** (2ц) 8.1. Сайжруулалт Байнгын сайжруулалт, Үл тохирол ба залруулах арга хэмжээ /ISO27001 стандартын 10-р бүлэг/ 8.2. Стандартын хяналт 8.3. Дасгал ажил болон хэлэлцүүлэг
	Модуль 3. Кибер халдлагын дадлага сургуулилт
	Хичээл 9: (2ц) 9.1. Халдлагыг тодорхойлох, халдлагын төрлүүд, хамгаалах, илрүүлэх, хариу үзүүлэх, засварлах алхмууд 9.2. Халдлагыг турших дасгал ажил 1: (Emotet Malware-

	н тухай болон хэрхэн хамгаалах талаар, Yara tool-г ашиглан сэжигтэй файлд шинжилгээ хийх (1 цаг), Nmap ашиглан нээлттэй порт болон үйлдлийн системийн хувилбарыг шалгах (10 мин), Password cracking (1 цаг), Heartbleed эмзэг байдлын талаар болон хэрхэн шалгах талаар (30 мин) , Eternal Blue эмзэг байдлыг ашиглан Windows үйлдлийн систем рүү exploit хийх (1 цаг)) 9.3. Хэлэлцүүлэг **Хичээл 10:** (2ц) 10.1. Халдлагад хариу үзүүлэх, засварлах, турших алхмууд 10.2. Халдлагыг турших дасгал ажил 2: (Web application, Burp suite ашиглан SQL injection халдлагыг турших (SQL login bypass, UNION, filter bypass болон Blind халдлагыг турших 1 цаг 30 мин), Wireshark ашиглан сүлжээний traffic-д анализ хийх, Cross-site Scripting халдлагыг турших (Reflected XSS болон Stored XSS 1 цаг 30 мин), Алсын хандалтын Pupy tool болон хэрхэн ашиглах талаар (30 мин), ARP poisoning халдлагыг туршин нууцлалгүй сүлжээний протоколуудад анализ хийх (HTTP, FTP)) 10.3. Хэлэлцүүлэг **Хичээл 11:** (2ц) 11.1. Халдлагад хариу үзүүлэх, засварлах, турших алхмууд 11.2. Халдлагыг турших дасгал ажил 3: (Linux үйлдлийн систем дээр backdoor үүсгэх туршилт (1 цаг), Shell-н тухай (Bind shell, Reverse shell) (30 мин), Linux болон Windows privilege escalation (Linux privilege escalation туршилт 1 цаг 30 мин), Active Director болон Kerberos Golden Ticket Attack-талаар (1 цаг), SSP халдлагын талаар болон турших (30 мин)) 11.3. Хэлэлцүүлэг **Хичээл 12:** (2ц) 12.1. Халдлагад хариу үзүүлэх, засварлах, турших алхмууд 12.2. Халдлагыг турших дасгал ажил 4: (PsExec tool-г ашиглан remote-р командуудыг ажиллуулах (30 мин), Schtasks командыг ашиглан remote-р scheduled task-г ажиллуулах (30 мин), RDP ашиглан remote port forwarding тохируулах (30 мин), APT attack-н талаар (10 мин), DNS tunneling халдлагын талаар (30 мин)) 12.3. Хэлэлцүүлэг