КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

УДИРДЛАГЫН АКАДЕМИ
ТӨРИЙН АЛБАНЫ СУРГУУЛЬ

MUST

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЧИГЛЭЛЭЭР МЭРГЭШҮҮЛЭХ СУРГАЛТ

- **Сургалтын үргэлжлэх хугацаа:** 2024 оны 05 дугаар сарын 27 - 29
- **Сургалтын хэлбэр:** Танхим
- **Сургалт зохион байгуулах газар:** 2024.05.27 /Удирдлагын Академийн хичээлийн төв байр 208 тоот танхим/

  2024.05.28-29 /ШУТИС-ийн хичээлийн 6-р байр, 315 тоот танхим/

Улаанбаатар хот
2024 он

Кибер Халдлага Зөрчилтэй Тэмцэх
Нийтийн Төв

1 СУРГАЛТЫН ЗОРИЛГО

- Төрийн байгууллагын мэдээллийн аюулгүй байдал хариуцсан мэргэжилтнүүдэд Монгол Улсын кибер аюулгүй байдлын тогтолцоо, хууль эрхзүй, зохицуулалтын орчны талаарх мэдлэг олгож, мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (МАБМТ)-г бий болгох, хэрэгжүүлэх, удирдах, хадгалах чиглэлээр ойлголттой болоход дэмжлэг үзүүлж, кибер сургуулилт хийн халдлагын үед авах арга хэмжээг хэрэгжүүлэх ур чадварыг эзэмшүүлнэ.

2 СУРГАЛТЫН ЗОРИЛТ

- Монгол Улсын кибер аюулгүй байдлын тогтолцоо, хууль эрхзүй, зохицуулалтын орчныг судлах
- Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог бий болгох, хэрэгжүүлэх, удирдах, хадгалах чиглэлээр ойлголттой болох
- Кибер сургуулилт хийж халдлагын үед авах арга хэмжээг хэрэгжүүлэх

3 СУРГАЛТЫН ҮР ДҮН

- Монгол Улсад мөрдөгдөж буй кибер аюулгүй байдлын хууль тогтоомжийг бүрэн судалсан байна.
- Мэдээллийн аюулгүй байдлын тогтолцооны талаар ойлголттой болсон байна.
- Халдлагын үед авах арга хэмжээг төлөвлөж, хэрэгжүүлэх чадвартай болсон байна.

СУРГАЛТЫН АГУУЛГА

09:00-09:30 СУРГАЛТЫН БҮРТГЭЛ

09:30-10:00 СУРГАЛТЫН НЭЭЛТ

Удирдлагын Академийн Төрийн албаны сургуулийн захирал, доктор, профессор
Д.Байгал

Кибер аюулгүй байдлын зөвлөлийн ажлын албаны дарга,
Монгол Улсын зөвлөх инженер
Ч.Золбаяр

2024 оны 05 сарын 27, Даваа гараг
Модуль 1. ХУУЛЬ ЭРХ ЗҮЙ, ЗОХИЦУУЛАЛТЫН ОРЧИН

ХУГАЦАА	ХИЧЭЭЛИЙН СЭДЭВ	СУРГАЛТЫН АРГА	БАГШ
10:00-11:30	Хичээл 1: Монгол улсын кибер аюулгүй байдлын тогтолцоо,Кибер аюулгүй байдлын тухай хууль	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	Кибер Халдлага Зөрчилтэй Тэмцэх Нийтийн Төвийн КХУСГазрын дарга Г.Гантуяа
11:35-13:05	Хичээл 2: Кибер аюулгүй байдлыг хангах нийтлэг журам, бусад хууль, дагалдах журмууд	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	ЦХХХЯ-ны КАББХЗГазрын Ахлах мэргэжилтэн Н.Балдансамбуу
13:05-14:05	**ИХ ЗАВСАРЛАГАА**		
14:05-15:35	Хичээл 3: Мэдээллийн аюулгүй байдлын бодлого боловсруулах үйл явц,Мэдээллийн аюулгүй байдлын бодлогын баримт бичгүүд, хэрэгжүүлэх арга замууд, Зарим улс оронд хэрэгжүүлдэг мэдээллийн аюулгүй байдлыг хангах стандартууд болон фрэймворкуудын тухай	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	Удирдлагын Академийн дэд профессор, доктор Б.Ганцэцэг
15:40-17:10	Хичээл 4: Мэдээллийн аюулгүй байдлын олон улсын эрх зүйн тогтолцооны тухай, Кибер гэмт хэргийн эрх зүйн зохицуулалтын орчин	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	Удирдлагын Академийн дэд профессор, доктор Б.Ганцэцэг

2024 оны 05 сарын 28, Мягмар гариг

Модуль 2. МЭДЭЭЛЛИЙН. АЮУЛГҮЙ БАЙДЛЫН УДИРДЛАГЫН ТОГТОЛЦОО (ISO27001:2022)

ХУГАЦАА	ХИЧЭЭЛИЙН СЭДЭВ	СУРГАЛТЫН АРГА	БАГШ
10:00-11:30	Хичээл 5: Хамрах хүрээ, эшлэл, нэр томьёо тодорхойлолт /ISO27001 стандартын 1-3 бүлэг/, Байгууллагын төлөв байдал /ISO27001 стандартын 4-р бүлэг/, Манлайлал Манлайлал ба үүрэг амлалт, Байгууллагын үүрэг хариуцлага, эрх мэдэл /ISO27001 стандартын 5-р бүлэг/	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Б.Даваасүрэн PECB ISO27001:2022 LA ISO27701:2019 LA
11:35-13:05	Хичээл 6: Төлөвлөлт Эрсдэл боломжид чиглэсэн арга хэмжээ Эрсдэлийг бууруулах арга, МАБ-ын зорилтод хүрэх төлөвлөгөө /ISO27001 стандартын 6-р бүлэг/, Дэмжлэг МАБ-ын шаардлагатай нөөц, мэдлэг, харилцаа холбоо, чадавх, баримтжуулсан мэдээлэл /ISO27001 стандартын 7-р бүлэг/	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Х.Уянгаа ISO27001:2022LA ISO9001:2015 IA
13:05-14:05	**ИХ ЗАВСАРЛАГАА**		
14:05-15:35	Хичээл 7: АжиллагааТөлөвлөлт ба хяналт, МАБ-ын эрсдэлийн үнэлгээ /ISO27001 стандартын 8-р бүлэг/, Гүйцэтгэлийн үнэлгээ Хяналт, хэмжилт, дүн шинжилгээ, үнэлгээ, дотоод аудит, УДШ /ISO27001 стандартын 9-р бүлэг/	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Б.Даваасүрэн PECB ISO27001:2022 LA ISO27701:2019 LA
15:40-17:10	Хичээл 8: Сайжруулалт Байнгын сайжруулалт, Үл тохирол ба залруулах арга хэмжээ /ISO27001 стандартын 10-р бүлэг/	Лекц, ярилцлага дасгал ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Б.Даваасүрэн PECB ISO27001:2022 LA ISO27701:2019 LA

2024 оны 05 сарын 29, Лхагва гариг

Модуль 3. КИБЕР ХАЛДЛАГЫН ДАДЛАГА СУРГУУЛИЛТ

ХУГАЦАА	ХИЧЭЭЛИЙН СЭДЭВ	СУРГАЛТЫН АРГА	БАГШ
10:00-11:30	Хичээл 9: Халдлагыг тодорхойлох, халдлагын төрлүүд, хамгаалах, илрүүлэх, хариу үзүүлэх, засварлах алхмууд.Халдлагыг турших дасгал ажил 1: (Emotet Malware-н тухай болон хэрхэн хамгаалах талаар, Yara tool-г ашиглан сэжигтэй файлд шинжилгээ хийх, Nmap ашиглан нээлттэй порт болон үйлдлийн системийн хувилбарыг шалгах, Password cracking, Heartbleed эмзэг байдлын талаар болон хэрхэн шалгах талаар, Eternal Blue эмзэг байдлыг ашиглан Windows үйлдлийн систем рүү exploit хийх)	Семинар, дадлага ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Ц.Энхтөр Ph.D., CEH
11:35-13:05	Хичээл 10: Халдлагад хариу үзүүлэх, засварлах, турших алхмууд Халдлагыг турших дасгал ажил 2: (Web application, Burp suite ашиглан SQL injection халдлагыг турших (SQL login bypass, UNION, filter bypass болон Blind халдлагыг турших), Wireshark ашиглан сүлжээний traffic-д анализ хийх, Cross-site Scripting халдлагыг турших (Reflected XSS болон Stored XSS), Алсын хандалтын Pupy tool болон хэрхэн ашиглах талаар, ARP poisoning халдлагыг туршин нууцлалгүй сүлжээний протоколуудад анализ хийх (HTTP, FTP))	Семинар, дадлага ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Ц.Энхтөр Ph.D., CEH
13:05-14:05	**ИХ ЗАВСАРЛАГАА**		
14:05-15:35	Хичээл 11: Халдлагад хариу үзүүлэх, засварлах, турших алхмууд Халдлагыг турших дасгал ажил 3: (Linux үйлдлийн систем дээр backdoor үүсгэх туршилт, Shell-н тухай (Bind shell, Reverse shell), Linux болон Windows privilege escalation (Linux privilege escalation туршилт), Active Director болон Kerberos Golden Ticket Attack-талаар, SSP халдлагын талаар болон турших)	Семинар, дадлага ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Ц.Энхтөр Ph.D., CEH И.Нуваанчимэд OSCP Авсртралын RackCorp-д МАБ-н шинжээч
15:40-17:10	Хичээл 12: Халдлагад хариу үзүүлэх, засварлах, турших алхмууд ашиглан remote-p scheduled task-г ажиллуулах, RDP ашиглан remote port forwarding тохируулах, APT attack-н талаар, DNS tunneling халдлагын талаар)	Семинар, дадлага ажил, хэлэлцүүлэг	ШУТИС, МХТС сургалтын төвийн багш Ц.Энхтөр Ph.D., CEH Х.Уянгаа ISO27001:2022 LA ISO9001:2015 IA
17:20-17:40	**СУРГАЛТЫН ХААЛТ (ДУРСГАЛЫН ЗУРАГ)**		