Канцелярия Премьер-Министра Республики Казахстан
Центр подготовки и повышения квалификации специалистов в области информационной безопасности

Министерство по инвестициям и развитию Республики Казахстан
Комитет связи, информатизации и информации
РГП «Государственная техническая служба»

Министерство образования и науки Республики Казахстан
Евразийский национальный университет им. Л.Н. Гумилева
Институт информационной безопасности и криптологии

ПРОГРАММА

III Международная научно-практическая конференция «Информационная безопасность в свете Стратегии «Казахстан - 2050»

15-16 октября 2015 года, г. Астана

Тема года:
"Информационная безопасность государств - членов Организации Договора о коллективной безопасности"

при поддержке

Университетская лига ОДКБ

Конференция проводится с целью обсуждения актуальных вопросов обеспечения информационной безопасности в рамках приоритетов Послания Президента Республики Казахстан - Лидера нации Нурсултана Назарбаева народу Казахстана «Стратегия «Казахстан-2050»: новый политический курс состоявшегося государства», а также является площадкой для конструктивного диалога представителей казахстанских и зарубежных ученых, государственных и бизнес-структур, направленного на реализацию Концепции информационной безопасности Республики Казахстан до 2016 года, утвержденной Указом Президента Республики Казахстан от 14 ноября 2011 года № 174.

Место проведения: ауд. 208 – Аудитория Первого Президента РК, Административный корпус, Евразийский национальный университет им. Л.Н. Гумилева, ул. К. Сатпаева, 2, г. Астана.

www.isc.enu.kz

ПРОГРАММНЫЙ КОМИТЕТ

Председатель:

Толымбеков Манат Исенулы – заведующий Отделом по защите государственных секретов Канцелярии Премьер-Министра РК

Сопредседатель:

Уразалина Акжунус Мухаметкалиевна (модератор) – директор Центра подготовки и повышения квалификации специалистов в области информационной безопасности Канцелярии Премьер-Министра РК

Тилеубеков Гани Утенович – заведующий Отделом информатизации и защиты информационных ресурсов Администрации Президента Республики Казахстан

Сыдыков Ерлан Батташевич – ректор Евразийского национального университета им. Л.Н. Гумилева, Республика Казахстан

Бигаринов Рустем Айдарбекович – заместитель заведующего Отделом информатизации и защиты информационных ресурсов Администрации Президента Республики Казахстан

Голобурда Дмитрий Васильевич – заместитель председателя Комитета связи, информатизации и информации Министерства по инвестициям и развитию РК

Абдикаликов Руслан Кенжебекович – директор департамента по контролю в области связи и информатизации Комитета связи, информатизации и информации Министерства по инвестициям и развитию РК

Есмамбетов Ерлан Кожабергенович – директор государственной технической службы Комитета связи, информатизации и информации Министерства по инвестициям и развитию РК

Шушин Владислав Олегович – эксперт по вопросам информационной безопасности и борьбы с киберпреступлениями, ОДКБ, Российская Федерация

Хотько Александр Николаевич – директор департамента информационных технологий Евразийской экономической комиссии

Тохтабаев Арнур Генрихович – PhD, эксперт в области информационной безопасности Центра подготовки и повышения квалификации специалистов в области информационной безопасности Канцелярии Премьер-Министра РК

Федоров Михаил Васильевич – Президент Университетской лиги ОДКБ, профессор, ректор Уральского государственного экономического университета, Российская Федерация

Нурбекова Жанат Кунапияновна – д.п.н., декан факультета информационных технологий ЕНУ им. Л.Н. Гумилева, Республика Казахстан

Бияшев Рустем Гакашевич – д.т.н., профессор, заведующий лабораторией информационной безопасности института информационных и вычислительных технологий МОН РК

Мазаков Талгат Жакупович – д.ф.-м.н., профессор, институт информационных и вычислительных технологий МОН РК

Конявский Валерий Аркадьевич – д.т.н., научный руководитель Всероссийского научно-исследовательского института проблем вычислительной техники и информатизации, Российская Федерация

Жангисина Гульнур Давлетжановна – д.п.н., проректор Центрально-азиатского университета, Республика Казахстан

Кунгожин Алмаз Мухамбетович – PhD, главный специалист по криптографическим вопросам ОЮЛ «Центр анализа и расследования кибератак», Республика Казахстан

Мусиралиева Шынар Женисбековна – PhD, доцент механико-математического факультета КазНУ им. аль-Фараби

Сейткулов Ержан Нураханович – к.ф.-м.н., директор института информационной безопасности и криптологии ЕНУ им. Л.Н.Гумилева

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Сыдыков Ерлан Батташевич – ректор Евразийского национального университета им. Л.Н. Гумилева

Уразалина Акжунус Мухаметкалиевна – директор Центра подготовки и повышения квалификации специалистов в области информационной безопасности Канцелярии Премьер-Министра РК

Сейткулов Ержан Нураханович – к.ф.-м.н, директор института информационной безопасности и криптологии ЕНУ им. Л.Н. Гумилева

Нурбекова Жанат Кунапияновна – д.п.н, декан факультета информационных технологий ЕНУ им. Л.Н. Гумилева, Республика Казахстан

Ташатов Нурлан Наркенович – к.ф.-м.н., заведующий кафедрой Вычислительной техники ЕНУ им. Л.Н. Гумилева

Атанов Сабыржан Кубейсинович – д.т.н., профессор факультета информационных технологий ЕНУ им. Л.Н. Гумилева

Сатыбалдина Дина Жагипаровна – PhD, доцент факультета информационных технологий ЕНУ им. Л.Н. Гумилева

Боранбаев Сейлхан Нарбутинович – д.т.н., профессор факультета информационных технологий ЕНУ им. Л.Н. Гумилева

Оспанов Руслан Маратович – старший преподаватель факультета информационных технологий ЕНУ им. Л.Н. Гумилева

15 октября
Аудитория Первого Президента РК (ауд. 208),
ЕНУ им. Л.Н. Гумилева

Время	Названия мероприятий
08:30-10:00	**Регистрация участников**
10:00-10:15	**Приветственное слово:** **Тилеубеков Гани Утенович,** заведующий отделом информатизации и защиты информационных ресурсов Администрации Президента Республики Казахстан; **Сыдыков Ерлан Батташевич,** ректор Евразийского национального университета им. Л.Н. Гумилева; **Толымбеков Манат Исенулы**, заведующий отделом по защите государственных секретов Канцелярии Премьер-Министра РК; **Голобурда Дмитрий Васильевич**, заместитель председателя Комитета связи, информатизации и информации Министерства по инвестициям и развитию РК; **Сейткулов Ержан Нураханович**, директор НИИ информационной безопасности и криптологии ЕНУ им. Л.Н.Гумилева. Презентация проекта Резолюции Конференции.

10:15 – 11:45 **Пленарные доклады: Информационная безопасность ОДКБ, компьютерная безопасность и современная криптография**

1. **Шушин Владислав Олегович**, советник Секретариата Организации Договора о коллективной безопасности, эксперт по вопросам информационной безопасности и борьбы с киберпреступлениями. Тема доклада «*Состояние и актуальные вопросы формирования системы информационной безопасности в интересах государств – членов Организации Договора о коллективной безопасности*»;

2. **Конявский Валерий Аркадьевич**, д.т.н., научный руководитель Всероссийского научно-исследовательского института проблем вычислительной техники и информатизации, Российская Федерация. Тема доклада «*Новая гарвардская архитектура - облачные компьютеры с вирусным иммунитетом*»;

3. **Тохтабаев Арнур Генрихович**, PhD, эксперт в области информационной безопасности ЦППК КПМ РК. Тема доклада «*Кибератаки нового поколения и перспективные решения*»;

4. **Франческо Сика (Francesco Sica),** PhD, профессор Назарбаев Университет, Республика Казахстан. Тема доклада «Elliptic curve cryptography».

11:45-12:15 **Кофе-брейк**

12:15-13:45 **1. Международная информационная безопасность: интеграция информационных систем**

1.1. Бияшев Рустем Гакашевич, д.т.н., профессор, заведующий лабораторией информационной безопасности института информационных и вычислительных технологий МОН РК. Тема доклада «*Некоторые пути повышения информационной безопасности*»;

1.2. Лунин Анатолий Васильевич, заместитель ответственного секретаря Технического комитета по стандартизации (ТК26) «Криптографическая защита информации», заместитель генерального директора ОАО «ИнфоТеКС», Российская Федерация. Тема доклада «*Вопросы формирования единого пространства доверия при международном электронном взаимодействии*»;

1.3. Кирюшкин Сергей Анатольевич, к.т.н., советник генерального директора ООО «Газинформсервис», Российская Федерация. Тема доклада «*Актуальные вопросы информационной безопасности в трансграничном пространстве доверия ЕАЭС*»;

1.4. Сулейменов Айдос Жумагельдиулы, директор департамента инфраструктурных решений, РГП «Государственная техническая служба», Республика Казахстан. Тема доклада «*Инфраструктура открытых ключей Республики Казахстан*»;

13:45-14:45 **Перерыв на обед**

14:45-17:00 **2. Национальные аспекты ИБ, вопросы реагирования на инциденты информационной безопасности**

2.1. Жангисина Гульнур Давлетжановна, д.п.н., профессор, проректор Центрально-азиатского университета, Республика Казахстан. Тема доклада «*Современные требования к национальной безопасности: информационный аспект*»;

2.2. Томашевич Алла, директор ООО «МОРЭЙН», Республика Беларусь. Тема доклада «*Оценка соответствия средств защиты информации и объектов информационных технологий требованиям Технических нормативно-правовых актов*»;

2.3. Кунгожин Алмаз Мухамбетович, PhD, главный специалист по криптографическим вопросам ОЮЛ «Центр анализа и расследования кибератак», Республика Казахстан. Тема доклада «*Необходимость модернизации Государственного стандарта Республики Казахстан 1073 – 2007 «Средства криптографической защиты информации. Общие технические требования»;*

2.4. Бияшев Рустем Гакашевич, Бегимбаева Енлик Ериковна, Нысанбаева Сауле Еркебулановна, Институт информационных и вычислительных технологий МОН РК. «*Формирование защищенного трансграничного информационного обмена в интегрированной системе*»;

2.5. Олжас Сатиев, Ильяс Аринов, Александр Гурин, ОЮЛ «Центр анализа и расследования

кибератак», Республика Казахстан. Тема доклада «*Практический кейс по информационной безопасности*»;

2.6. Жакупов Жанат Мейрамович, начальник Службы реагирования на компьютерные инциденты РГП «Государственная техническая служба». Тема доклада «*Взаимодействие при реагировании на инциденты информационной безопасности*».

Выступления по внесению предложений в Резолюцию Конференции по итогам дня. Дискуссия.

17:00-18:00 **Фуршет**

16 октября

Аудитория № 303, УАК ЕНУ им. Л.Н.Гумилева

10:00-12:30 **3. Математические, компьютерные и технические аспекты информационной безопасности**

3.1. Мусиралиева Шынар Женисбековна, механико-математический факультет КазНУ им. аль-Фараби. Тема доклада «*О проектных решениях для современных технических систем безопасности*»;

3.2. Магзом Мирас, **Нысанбаева Сауле Еркебулановна,** Институт информационных и вычислительных технологий МОН РК. Тема доклада «*Моделирование нетрадиционного алгоритма шифрования с применением схемы Фейстеля*»;

3.3. Сейткулов Ержан Нураханович, Оспанов Руслан Маратович, Майманов Едил Муратович, факультет информационных технологий ЕНУ им. Л.Н.Гумилева, НИИ информационной безопасности и криптологии ЕНУ им. Л.Н.Гумилева, ТОО «Information Services Group». Тема доклада «*Сервис шифрования данных на заданное время*»;

3.4. Дюсенбаев Дилмуханбет Самуратович, **Капалова Нұрсұлу Алдажарқызы**, Институт информационных и вычислительных технологий МОН РК. Тема доклада «*Позициялық емес полиномдық санау жүйесіне негізделген шифрлеу алгоритмдеріне сызықтық криптоалдауды қолдану*».

3.5. Тохтабаев Арнур Генрихович, Антон Копейкин, ТОО «T&T Security», Республика Казахстан. Тема доклада «*tLab: платформа для автономного анализа поведения программ и идентификации зловредных функциональностей*»;

3.6. Ташатов Нурлан Наркенович, Сатыбалдина Дина Жагипаровна, Мишин Виталий Алексеевич, Исайнова Алия Насиповна, Факультет информационных технологий, НИИ информационной безопасности и криптологии ЕНУ им. Л.Н.Гумилева. Тема доклада «*Оптимизация параметров работы каскадных схем на основе многопороговых декодеров недвоичных сверточных кодов*»;

3.7. Золотарев Валерий Владимирович, Овечкин Геннадий Владимирович, Ташатов Нурлан Наркенович, Институт космических исследований РАН, Москва, РФ, ЕНУ им. Л.Н.Гумилева. Тема доклада «*Применение принципа дивергенции при декодировании свёрточных кодов*».

Инициативные доклады. Заключительные выступления по внесению предложений в Резолюцию Конференции. Дискуссия.

12:30-13:30 **Перерыв на обед**

13:30-14:00 **Закрытие конференции;**
Общее фотографирование участников конференции.

14:00-17:00 **Культурная программа по городу для гостей конференции**

Доклады
www.isc.enu.kz

1. **Айжамбаева С.Ж., Бакей Д.К.** *Применение современных информационных систем на автомобильном транспорте*

2. **Акашаев Н.А., Сатыбалдина Д.Ж.** *Протокол обмена секретным ключом, основанный на синхронизации двух древовидных машин четности*

3. **Актаева А., Илипбаева Л.Б., Баймуратов А., Галиева Н.** *Информационная безопасность: квантовые технологии*

4. **Александров А. В.** *О семействе рюкзачных блочных шифров*

5. **Альмухамбетов С.** *Защита программного обеспечения*

6. **Арипов М.М., Курьязов Д.М.** *Об одном алгоритме ЭЦП с увеличенной стойкостью*

7. **Арипов М.М., Туйчиев Г.Н.** *Development block encryption algorithm based networks IDEA16–2 and RFWKIDEA16–2 using the transformation of encryption algorithm AES*

8. **Ахметов Б.С., Корченко А.Г., Сейлова Н.А., Гнатюк С.А., Алимсеитова Ж.К.** *Инфокоммуникаялық жүйелерде қауіпсіздік деңгейін жоғарлату мақсатында кванттық технологияларды қолдану*

9. **Баймульдин М.К., Каримова А., Абилдаева Г.Б.** *Ақпараттық салада жұмыс істейтін ұйымдарда құпия ақпаратты қорғау*

10. **Баймульдин М.К., Савченко Н.К., Шакирова Ю.К., Абилдаева Г.Б.** *Использование систем планирования бизнес-ресурсов с целью повышения потенциала предприятия*

11. **Барлыбаев А.Б., Сабыров Т.С.** *Информационная безопасность в Smart - University*

12. **Бердибаев Р.Ш., Абулхасимова М.Б., Жаманкулова А.А.** *Возможности применения искусственного интеллекта в биометрических системах аутентификации*

13. **Бердибеков А.Т., Доля А.В.** *Некоторые аспекты защиты информации в системах электронного документооборота*

14. **Бияшев Р.Г., Нысанбаева С.Е., Бегимбаева Е.Е.** *Формирование защищенного трансграничного информационного обмена в интегрированной системе*

15. **Боранбаев С.Н., Тасмагамбетов О.К., Сейткулов Е.Н.** *Требования при проектировании информационной системы поддержки правоохранительной деятельности*

16. **Боранбаев С.Н., Тасмагамбетов О.К., Сейткулов Е.Н.** *Структура и функциональные задачи информационной системы поддержки правоохранительной деятельности*

17. **Гафуров Х.** *Стегоанализ в среде программы Mathcad11*

18. **Джамбеков А.М.** *Нечеткое ситуационное управление процессами защиты информации нефтегазового предприятия*

19. **Доля А.В., Бердибеков А.Т.** *Защита информации в телекоммуникационных системах*

20. **Жангисина Г.Д.** *Современные требования к национальной безопасности: информационный аспект*

21. **Жук А.П., Осипов Д.Л., Гавришев А.А.** *Анализ методов оценки защищенности беспроводной сигнализации*

22. **Жумагулова С.К., Турсынгалиева Г.Н.** *Создание программного комплекса криптографического преобразования конфиденциальной информации методом прямой замены*

23. **Заурбек А., Ахметов Б.С., Джурунтаев Д.З, Сейлова Н.А.** *Схема генератора акустического шума для защиты речевой информации от скрытой звукозаписи*

24. **Золотарев В.В., Овечкин Г.В., Ташатов Н.Н.** *Применение принципа дивергенции при декодировании свёрточных кодов*

25. **Ибраев Н.С.** *Информационная безопасность фактор успешного планирования военных (специальных) мероприятий коллективных сил оперативного реагирования Организации Договора о коллективной безопасности*

26. **Исмоилов Д.** *Об одном применении арифметики в криптографии*

27. **Капалова Н.А., Дюсенбаев Д.С.** *Позициялы емес полиномды санау жүйесіне сызықтық криптоанализды қолдану*

28. **Капослёз Г.В.** *Анализ информационного пространства как среды реализации информационного влияния*

29. **Касенов Т.А.** *Роль военной полиции США в обеспечении информационной безопасности*

30. **Кацалап В.А.** *Предварительное планирование информационной операции*

31. **Клиновой Д.В., Рогов П.Д., Белокур Н.А.** *Проблемы информационной безопасности процесса децентрализации управления природными ресурсами государства*

32. **Корченко А.Г., Казмирчук С.В., Алимсеитова Ж.К., Жекамбаева М.Б.** *Программное средство оценки рисков информационной безопасности COBRA*

33. **Корченко А.Г., Казмирчук С.В., Ахметова С.Т., Жекамбаева М.Б.** *Программное средство оценки рисков информационной безопасности CRAMM*

34. **Куламбаева К.К.** *Некоторые гуманитарные аспекты информационной безопасности*

35. **Кулатаев С.А.** *Роль информационного противоборства в современных конфликтах*

36. **Курымбаев С.Г., Бакей Д.К.** *Значение применения информатизации на транспорте*

37. **Курьязов Д.М., Саттаров А.Б.** *Метод построения алгебраической системы уравнений, описывающей S – блок*

38. **Лукичев В.Ф.** *Принципы создания единой системы национальной безопасности*

39. **Лунин А.В.** *Вопросы формирования единого пространства доверия при международном электронном взаимодействии*

40. **Метлинов А.Д.** *Скоростные характеристики симметричной рюкзачной криптосистемы с общей памятью. NIST – тестирование.*

41. **Мусиралиева Ш.Ж., Абдаким Г.** *Заманауи техникалық қауіпсіздік жүйелері үшін проектілік шешімдер*

42. **Нурланова Б.М., Жумагулова С.К., Алибиев Д.Б.** *Ақпаратты қорғаудың криптографиялық әдістерін қолданудың кейбір аспектілері*

43. **Нысанбаева С.Е., Магзом М.М.** *Моделирование нетрадиционного алгоритма шифрования с применением схемы Фейстеля*

44. **Полежаев П.Н.** *Реализация алгоритма межсетевого экрана для облачных систем с использованием технологии программно-конфигурируемых сетей*

45. **Рогов П.Д., Белокур Н.А., Ворович Б.А.** *Стратагемное мышление как основа достижения целей в борьбе за национальные интересы*

46. **Сарычев Ю.А., Сницаренко П.Н.** *Условия внедрения государственной системы обеспечения информационной безопасности Украины в военной сфере*

47. **Сарычев Ю.А., Ткаченко В.А.** *Проблемы обеспечения информационной безопасности войск в современных условиях*

48. **Сейлова Н.А., Алимсеитова Ж.К., Оган А., Балтабай А.** *Применение биометрической аутентификации по отпечатку пальца в подготовке специалистов*

49. **Сейткулов Е.Н., Боранбаев С.Н., Давыдов Г.В.** *Исследование вероятности появления букв в текстах на казахском языке*

50. **Сейткулов Е.Н., Боранбаев С.Н., Давыдов Г.В.** *Разработка алгоритма синтеза речеподобных сигналов на казахском языке*

51. **Сейткулов Е.Н., Оспанов Р.М., Майманов Е.М.** *Сервис шифрования данных на заданное время*

52. **Спирина Е.А., Смирнова М.А., Самойлова И.А., Мирзабаева В.Д.** *Подготовка студентов IT-специальностей в сфере информационной безопасности в Карагандинском государственном университете*

53. **Стюгин М.А., Паротькин Н.Ю., Золотарев В.В.** *Технология защиты информации с применением движущейся цели в задачах безопасной адресации узлов компьютерной сети*

54. **Султанов Т.Т., Бельгибеков Н.А.** *Автоматизированные системы управления и информационные технологии в Вооруженных Силах Республики Казахстан*

55. **Ташатов Н.Н., Сатыбалдина Д.Ж., Мишин В.А., Исайнова А.Н.** *Оптимизация параметров работы каскадных схем на основе многопороговых декодеров недвоичных сверточных кодов*

56. **Ташатов Н.Н., Тургинбаева А.С., Серикова Н.С.** *Проблемы защиты информации в информационных системах в РК.*

57. **Тельный А.В.** *О возможности повышения точности позиционирования подвижного объекта при навигационных измерениях*

58. **Токсоналиева Р.М.** *Современные угрозы информационно – психологической безопасности государств - членов ОДКБ*

59. **Толеуханова Р.Ж.** *Аналитический метод восстановления цифровых сигналов изображений в базисе Уолша*

60. **Туйчиев Г.Н.** *The encryption algorithms GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4*

61. **Устинова Л.В., Смирнова М.А., Самойлова И.А.** *Активные методы воздействия в сети*

62. **Червяков Н.И., Шалалыгина И.В.** *Анализ метода и алгоритма основного модулярного деления.*

63. **Червяков Н.И., Шалалыгин Д.Г.** *Анализ методов коррекции ошибок в СОК.*

64. **Червяков Н.И., Шалалыгин Д.Г., Шалалыгина И.В.** *Краткая характеристика системы остаточных классов.*

65. **Черногорова Ю.В.** *Исследование алгоритмов перевода чисел из системы остаточных классов в позиционную систему счисления*