

## СОДЕРЖАНИЕ

1. Байғабыл Ұ.Д. АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУДЫ СТАНДАРТТАР ТАЛАПТАРЫ БОЙЫНША БАҒАЛАУДЫҢ ЭКСПЕРТТІК ЖҮЙЕСІ .....	3
2. Дутпаева М.К. АҚПАРАТТЫ ҚОРҒАУДЫҢ КРИПТОГРАФИЯЛЫҚ ӘДІСТЕРІ .....	9
3. Муратбеков М.М., Алтынбек С.А., Абылаева А.М., Тургинбаева А.С. ТАҚ РЕТТІ ЭЛЛИПТИКАЛЫҚ ҚИСЫҚТАРДЫҢ НЕГІЗІНДЕ ДИФФИ-ХЕЛЛМАН КРИПТОЖҮЙЕСІН ҚҰРУ .....	14
4. Мұса А.Ш. СРУРТОН БЛОКТЫҚ ШИФРЛЕУІНЕ МБҚ- МАТРИЦАСЫ .....	18
5. Омаров Б.С., Актаева А.У., Әшімақын Ж.Т. НЕЙРОЖЕЛІЛІК ТЕХНОЛОГИЯ: АҚПАРАТТЫҚ РЕСУРСТАРҒА ЖАСАЛАТЫН ЖЕЛІЛІК ШАБУЫЛДАРДЫ АНЫҚТАУ .....	20
6. Актаева А., Мурзағалиева Н. НЕЙРОСЕТЕВЫЕ ТЕХНОЛОГИИ КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ .....	23
7. Александров А.В., Метлинов А.Д., Зимников А.С. О СЕМЕЙСТВЕ РЮКЗАЧНЫХ БЛОЧНЫХ ШИФРОВ С ОБЩЕЙ ПАМЯТЮ И ПЛОТНОСТЮ УКЛАДКИ БОЛЬШЕ ЕДИНИЦЫ И ХЕШ-ФУНКЦИЙ НА ИХ ОСНОВЕ .....	31
8. Бегимбаева Е.Е. О ЗАЩИЩЕННОМ ТРАНСГРАНИЧНОМ ИНФОРМАЦИОННОМ ОБМЕНЕ .....	36

9.	Бекбулатов Е.Л., Бекбулатов Е.Р., Мусиралиева Ш.Ж. О ПРОЕКТНЫХ РЕШЕНИЯХ ДЛЯ ТЕХНИЧЕСКОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ПЭРКo .....	40
10.	Бияшев Р.Г., Нысанбаева С. Е. ПОСТРОЕНИЕ И АНАЛИЗ МОДУЛЯРНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ....	45
11.	Дюсенбина А.Б., Тэн В.Д. ЛИНЕЙНЫЙ ШИФР С НАПОЛНЕНИЕМ И СЖАТИЕМ .....	64
12.	Жетписов С.Н. ДЕМОГРАФИЧЕСКАЯ БЕЗОПАСНОСТЬ .....	68
13.	Золотарев В.В., Сатыбалдина Д.Ж., Ташатов Н.Н., Сейткулов Е.Н. ХАРАКТЕРИСТИКИ МНОГОПороГОВОГО ДЕКОДИРОВАНИЯ .....	88
14.	Кабылханов А. Б. СТОЙКОСТЬ АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89 .....	98
15.	Капалова Н. А. АСИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ НА БАЗЕ МОДУЛЯРНОЙ АРИФМЕТИКИ .....	103
16.	Касабеков С.А., Жангисина Г.Д., Муналбаева Н.Р., Сабырова Ж.К. ОПЫТ ЗАРУБЕЖНЫХ ГОСУДАРСТВ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .....	107
17.	Кобзарев В.А. МЕТОДЫ СДЕРЖИВАНИИ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА .....	113
18.	Оспанов Р.М. КАТАЛОГ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ .....	119
19.	Рог О. А. ОСНОВЫ ФУНКЦИОНИРОВАНИЯ МОДЕЛИ МНОГОКРИТЕРИАЛЬНОЙ СИСТЕМЫ РАЗГРАНИЧЕНИЯ И КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ .....	134

20. Садвакасова К.Ж., Закирова А.Б., Шуйтенов Г.Ж. ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .....	139
21. Сейткулов Е.Н., Тохтабаев А. ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ И ПРОБЛЕМА БЕЗОПАСНОСТИ: АУТСОРСИНГ ВЫЧИСЛИТЕЛЬНО-СЛОЖНЫХ ЗАДАЧ С СЕКРЕТНЫМИ ДАННЫМИ .....	144
22. Сейткулов Е.Н., Боранбаев С.Н., Ергалиева Б.Б., Давыдов Г.В. ИССЛЕДОВАНИЯ ВОЗБУЖДЕНИЯ ВИБРАЦИЙ ОГРАЖДАЮЩИХ КОНСТРУКЦИЙ ДЛЯ ЦЕЛЕЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ .....	152
23. Сейткулов Е.Н., Боранбаев С.Н., Ергалиева Б.Б., Давыдов Г.В. МЕТОД ФОРМИРОВАНИЯ КОМБИНИРОВАННЫХ МАСКИРУЮЩИХ СИГНАЛОВ .....	175
24. Таниева Б.А. ПРИМЕНЕНИЕ СИСТЕМЫ SCADA ДЛЯ ОБЕСПЕЧЕНИЯ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИИ .....	197
25. Токсоналиева Р.М. К ВОПРОСУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В ЦЕНТРАЛЬНОАЗИАТСКОМ РЕГИОНЕ ..	200
26. Туйчиев Г.Н. ГЕНЕРАЦИЯ СТОЙКИХ БУЛЕВЫХ ФУНКЦИЙ НА ОСНОВЕ КОНСТРУКЦИИ НИБЕРГ И ЕЕ ПРИМЕНЕНИЕ	205
27. Хакимов Р.А. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ФОРМИРОВАНИЯ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ ПОЛИНОМИАЛЬНОЙ МОДУЛЯРНОЙ АРИФМЕТИКИ .....	216
28. Abduraimova V.K. TECHNICAL FACILITIES DEVELOPMENT AND DESIGN METHODS FOR INFORMATION SECURITY IN DISTRIBUTED INFORMATION SYSTEMS .....	221

29. Kasabekov S., Zhangissina G., Munalbaeva N., Zholymbet B.Sh. CRYPTOGRAPHIC METHODS OF INFORMATION SECURITY	226
30. Sadvakasova K., Kalimbetov A. REAL-TIME OPERATING SYSTEM FOR SAFETY CRITICAL SYSTEMS. RTAI .....	231
31. Tokhtabayev A.G., Seitkulov Y., Skormin V.A. RUN-TIME DETECTION OF INTER AND INTRA PROCESS MALICIOUS FUNCTIONALITIES THROUGH COLORED PETRI NETS .....	236
32. Zhangisina G., Kasabekov S., Orazhanov A., Usen A., Esetov Sh. INFORMATION SECURITY OF KAZAKH AIRLINES .....	276