Краткая информация о проекте

Наименование	AP19174716 «Разработка системы поддержки принятия решений на основе байесовских сетей для повышения эффективности выявления вторжений в компьютерные системы» (0123РК00972)
Актуальность	Анализ существующих систем выявления вторжений и системах сбора и корреляции событий (Security Information and Event Management, SIEM) показывает тенденцию к интеллектуализации процессов анализа данных, которые используются для идентификаций действий потенциальных нарушителей информационной безопасности (ИБ) и кибербезопасности (КБ) объектов информатизации (ОБИ). Это особенно стало заметно в условиях повышения количества и качества злонамеренных действий, направленных на дестабилизацию процесса функционирования компьютерных и информационных систем. Проведенный анализ математических методов для современных систем выявления вторжений (СВВ) в информационно-коммуникационные сети ОБИ обнаружил ряд как их преимуществ, так и недостатков. На сегодняшний день существующие СВВ не всегда не эффективны против новых типов вторжений, особенно в ситуациях, которые характеризуются слабо структурированными данными о признаках атак или нечетко определенными критериями в соответствующей задаче распознавания новых угроз. Поэтому разработка соответствующих методов идентификации аномальных состояний для СВВ за счет интеграции в их состав интеллектуальных систем поддержки принятия решений (СППР) с целью расширения функциональных возможностей стороны защиты, позволит этим СВВ быть более действенными по выявлению новых типов кибератак. Исходя из существующего явного противоречия между увеличением уровня кибернетических угроз безопасности ОБИ и повышением интенсивности внешних вредоносных воздействий с одновременным повышением требований к КБ, важной научно-технической задачей является дальнейшее развитие существующих и разработка новых методов и моделей для интеллектуальных СППР в условиях слабо структурированных данных о признаках и выявленных аномалиях в ИС. Как показано многими теоретиками в области изучения ИБ и КБ, одним из наиболее перспективных направлений идентификации злоупотреблений являются методы, адаптированные к анализу ситуаций, которые связаны с распознаванием длительных кибератак, не сопровождающихся явными признаками. К таким методам в полной мере относятся методы, основанные на байесовских сетях (БС) и байесовских классификаторах, что и определяет актуальность темы нашего исследования.
Цель	Цель проекта – повышение качества оценок вероятности реализации угроз злоумышленника ОБИ путем разработки

	подхода, основанного на применении байесовских сетей в сложно формализованных нетипичных ситуациях реализации многоэтапных целевых кибератак на ОБИ.
Задачи	Для достижения поставленной цели должны быть решены следующие взаимосвязанные задачи: 1) провести анализ существующих систем выявления вторжений и систем сбора и корреляции событий (Security Information and Event Management, SIEM) 2) разработать шаблоны БС и новые модели для вычислительного ядра СППР в ходе прогнозирования угроз и этапов вторжения в информационно-коммуникационные сети (ИКС) объектов информатизации; 3) дополнить вероятностные модели выявления сетевых вторжений на основе применения динамических БС; 4) разработать и протестировать СППР в задачах анализа данных на основе использования БС.
Ожидаемые и достигнутые результаты	Разрабатываемые в рамках проекта шаблоны БС для вычислительного ядра СППР в ходе прогнозирования угроз и этапов вторжения в ИКС ОБИ, позволят аналитикам ИБ с помощью СППР оперировать множеством случайных переменных и определять вероятность реализации угроз или конкретного этапа вторжения в ИКС ОБИ при заданных условиях. По сравнению с аналогичными работами в нашем проекте будут дополнены вероятностные модели выявления сетевых вторжений на основе применения динамических БС. Кроме того, предлагаемый подход дает возможность не только учитывать основные этапы вторжений, но и более обоснованно принимать решения на основе применения как типовых шаблонов вторжений, так и вновь синтезируемых шаблонов. Все шаблоны и модели составляют вычислительное ядро системы поддержки принятия решений в ходе выявления вторжений, которые могут на разных этапах характеризоваться слабоструктурированными признаками.
Имена и фамилии членов исследовательской группы с их идентификаторами (Scopus Author ID, Researcher ID, ORCID, при наличии) и ссылками на соответствующие профили	1. Ыдырышбаева Мөлдір Базарханкызы, магистр естественных наук, Индекс Хирша – 1, ORCID: https://orcid.org/0000-0002-5680-5444, Scopus Author ID: 57222863896 2. Ахметов Бахытжан Сражатдинович, профессор, , д.т.н, Индекс Хирша – 7, ResearcherID: ABI-3310-2020, ORCID: https://orcid.org/0000-0001-5622-2233, Scopus Author ID: 56829370400
Список публикаций со ссылками на них	
Информация о патентах	-