УДК 004.056.5+004.81
ББК 32.972.5

DOI 10.47475/2618-9852-2022-17310

КОГНИТИВНАЯ БЕЗОПАСНОСТЬ: ИССЛЕДОВАНИЕ КОГНИТИВНОЙ НАУКИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Д. О. Сулейманова, Т. Р. Магомаев

Грозненский государственный
нефтяной технический университет
имени академика М. Д. Миллионщикова,
Грозный, Россия.

В настоящее время быстрые темпы технологических изменений приводят к скорому появлению все новых угроз, порождающих необходимость в обновлении и разработке более эффективных сценариев обеспечения кибербезопасности. Принимая во внимание обстоятельства, в статье исследуются особенности и проблемы внедрения когнитивных технологий в модель обеспечения информационной безопасности.

Ключевые слова: *когнитивная безопасность, кибербезопасность, когнитивные науки.*

COGNITIVE SECURITY: A STUDY OF COGNITIVE SCIENCE IN CYBERSECURITY

D.O. Suleymanova, T.R. Magomaev

Grozny State Oil Technical University
named after academician M. D. Millionshchikov, Grozny, Russia

Nowadays, IoT, cloud computing, mobile and social networks are generating a transformation in social processes. Nevertheless, this technological change rise to new threats and security attacks that produce new and complex cybersecurity scenarios with large volumes of data and different attack vectors that can exceeded the cognitive skills of security analysts. In this context, cognitive sciences can enhance the cognitive processes, which can help to security analysts to establish actions in less time and more efficiently within cybersecurity operations. The perspectives in the field of cybersecurity regarding cognitive sciences are find solutions to enhanced the capacities related to the human factor, especially in complex systems that are generated with the use of technologies such as cloud, mobile, IoT and social networks that produce large amounts of information. Taking into account the circumstances, the article examines the features and problems of the introduction of cognitive technologies into the information security model.

Keywords: *cognitive security, cybersecurity, cognitive sciences.*

Согласно прогнозам Forbes и Gartner, правительственных организаций, таких как NSA[1], NIST[2] и Европейской комиссии, проблемами в области кибербезопасности являются:

• Алгоритмы в области искусственного интеллекта (ИИ), использующие организационные или персональные данные для генерации прогнозов. Эти данные могут быть конфиденциальными, поэтому необходимо усилить механизмы защиты информации, особенно для персональных данных. В ИИ злоумышленники могут подделать данные, влияющие на результаты, и таким образом фальсифицировать их. Неправильно функционирующий ИИ может использоваться для нападения на системы или против людей. Некоторые проблемы в области кибербезопасности, связанные с использованием искусственного интеллекта, заключаются в следующем:

- конфиденциальность информации, используемой в ИИ;
- целостность информации, используемой в ИИ;
- неправильное использование искусственного интеллекта.

[1] Агентство национальной безопасности (англ. National Security Agency).

[2] Национальный институт стандартов и технологий США (англ. The National Institute of Standards and Technology).

• Программы-вымогатели, ставшие мощным оружием киберпреступности. Только в период с 2020 по 2022 года было выявлено около 1,16 млрд. случая атак [10]. При этом потери измеряются миллиардами долларов. Некоторые проблемы в области кибербезопасности, связанные с этим аспектом, заключаются в следующем:
- выявление шаблонов программ-вымогателей;
- установите процессы согласования для предотвращения распространения программ-вымогателей;
- определение схем защиты данных.

• Блокчейн. Использование криптовалюты потенциально рассматривается как вариант оптимизации процессов электронных переводов в банковской сфере, здравоохранении или бизнесе. Однако на уровне безопасности существуют некоторые проблемы:
- увеличение времени восстановления в случае сбоя за счет децентрализованного администрирования;
- обеспечение правильного функционирования контрактов;
- обеспечение инфраструктуры, поддерживающей блокчейн.

• Безопасность интернета вещей. Существует угроза столкновения со следующими проблемами в IoT, связанными с кибербезопасностью:
- Безопасная связь между устройствами интернета вещей.
- Авторизация и аутентификация устройств.
- Конфиденциальность и целостность данных.
- Управление обновлениями устройств.
- Кража личных данных устройств.

• Безопасность бессерверных приложений. Контейнеры в облаке позволяют снизить эксплуатационные расходы и ускорить сроки доставки пользователю, при использовании моделей сервисов, доступных в облаке. Некоторыми из угроз безопасности в данном случае являются:
- нарушение аутентификации;
- незащищенные бессерверные конфигурации;
- неадекватный мониторинг;
- зависимость от ненадежных третьих сторон.

В условиях существования больших объемов данных и разрозненных между собой возможных векторов атак, возрастают требования к когнитивным навыкам специалистов по безопасности. В таком контексте когнитивные науки могут улучшить процессы, позволяющие аналитикам разрабатывать сценарии действий за меньшее время и более эффективно в рамках операций по обеспечению кибербезопасности.

Когнитивные науки определяются как междисциплинарное научное исследование психологии, компьютерных наук, лингвистики, философии и неврологии, обеспечивающих понимание человеческого разума [6]. Их применение в области кибербезопасности позволяет осуществлять взаимосвязь между процедурами, методами обеспечения безопасности, знаниями, полученными с помощью компьютерных систем, и опытом специалистов по безопасности на основе выполняемых ежедневных задач. Сотрудничество между людьми и машинами, применение статистических методов, использование машинного обучения и Больших данных может позволить улучшить и расширить сценарии реагирования на угрозы информационной безопасности. Перспективы в области кибербезопасности в отношении когнитивных наук заключаются в поиске решений для расширения возможностей, связанных с человеческим фактором, особенно в сложных системах, которые создаются с использованием таких технологий, как облачные, мобильные и социальные сети, которые производят большие объемы информации. В настоящее время в научной сфере становится необходимым проанализировать возможности и пути внедрения когнитивных наук в модели кибербезопасности в целях расширения человеческих возможностей для выполнения задач, требующих использования когнитивных навыков.

Модель безопасности с внедренными в нее когнитивными технологиями направлена на интеграцию различных решений в целях улучшения операций по обеспечению кибербезопасности. В случае использования искусственного интеллекта в кибербезопасности аналитик создает базу знаний, которая в дальнейшем используется для принятия наилучшего решения для реагирования на атаки; если инцидент ранее не был занесен в каталог, или если база знаний ограничена, или если конкретные задачи четко не определены, решение не сможет адекватно достичь поставленных целей. Такая ситуация может привести к непредсказуемым последствиям, которые в определенных случаях могут быть критически опасными. Если качество данных не проверяется, специалист по безопасности может принимать решения на основе недостоверной информации; эта ситуация может привести к негативным результатам [1].

Ниже приведены минимальные характеристики, которые должны обеспечивать получение качественных данных:
• последовательность;
• точность;
• полнота;
• возможность проверки;

• упорядоченность.

Оперативные действия в процессе реагирования на инциденты, как правило, являются длительными, утомительными и требуют от специалистов по кибербезопасности отточенных когнитивных навыков. Человеческие ограничения при обработке больших объемов данных и факторы, влияющие на когнитивные способности человека, такие как стресс и эмоции, могут снизить точность и эффективность реагирования на угрозы [9]. Некоторые альтернативы для поддержки процесса реагирования на инциденты путем автоматизации задач могут устранить это ограничение. Рассмотрим некоторые из них.

Динамические модели: ограничение статических моделей при реагировании на инциденты безопасности заключается в том, что они основаны на наборе возможных ответов, предопределенных аналитиком безопасности, поэтому, если существует неизвестный вариант атаки, модель не сможет его предсказать. Тогда главным преимуществом динамических моделей является их адаптивность к изменениям в цифровой среде.

Модели когнитивных карт: когнитивная карта основана на создании матриц в соответствии с заключениями команды безопасности, в зависимости от различных проанализированных ими альтернатив относительно того, как разрешить инцидент. Шаги, которые необходимо предпринимать для формирования решения, включают [7]:

- генерацию сценария атак;
- создание вероятностных вариантов реагирования на инциденты;
- выбор наиболее подходящих вариантов.

Модель теории игр: использование теории игр основано на установлении двух ролей (атаки и защиты) для прогнозирования возможных сценариев атак. Для реализации теории игр могут применяться:

- равновесие Нэша;
- стохастические модели;
- Байесовское обучение.

Многоагентные модели: многоагентная система (MAS) выполняет задачи по решению проблем, связанных с обработкой инцидентов. Целью является обеспечение автономной и децентрализованной архитектуры, основанной на следующих действиях:

- идентификация и регистрация;
- категоризация и расстановка приоритетов;
- диагностика и масштабирование;
- разрешение и восстановление элементов;
- закрытие инцидента.

Аналитик по безопасности объединяет опыт и практические знания для оценки и интерпретации наблюдений, чтобы выдвинуть гипотезу о событиях, которые могут быть возможными атаками. Для этого требуется обработать несколько источников данных и информации и установить корреляцию между ними и цифровой средой. Аналитик по безопасности должен отвечать за следующие действия [3]:

- мониторинг сети;
- выявление угроз;
- исправление уязвимости.

Для выполнения этих действий аналитик выполняет следующие когнитивные процессы:

- идентификация;
- наблюдение;
- генерация гипотез;
- исследование гипотез.

На конференции RSA (международная конференция по информационной безопасности) в 2017 году были озвучены когнитивные задачи, которые аналитик должен выполнять при расследовании инцидентов безопасности. Они перечислены ниже:

1. Идентификация:

- просмотр данных об инцидентах;
- исследование события по интересующим аспектам.

2. Наблюдение:

- развертывание данных с целью поиска нетипичных значений;
- расширение поиска.

3. Генерация гипотезы;

4. Исследование гипотезы.

- расследование инцидента;
- обнаружение потенциально зараженных участков;
- классифицирование инцидента на основе знаний, полученных на этапе расследования угрозы;
- анализ на основе профиля атаки;
- анализ карты распространения атаки.

Когнитивные способности, необходимые аналитику безопасности для выполнения вышеперечисленных задач, включают:

- стратегическое мышление;
- изобретательный подход;
- ответственность;
- обучаемость.

В эпоху цифровых технологий и усложнения угроз и атак их серьезность возросла, а их возникновение приводит к появлению миллионов данных, требующих высокой производительности обработки. На различных уровнях кибербезопасности роль человека является важным фактором, который не может быть сведен к минимуму только за счет внедрения решений автоматизации, но также требует повышения когнитивных способностей аналитика безопасности.

Учитывая важность того, что Большие данные и искусственный интеллект интегрируются в когнитивную систему, рекомендуется использовать методологию CRISP-DM для поддержания надлежащего качества данных [2]. Эта методология также позволяет создать процесс моделирования, основанный на анализе данных. При этом когнитивным системам все еще не хватает должного уровня самосознания, поэтому они не способны полностью самостоятельно понимать положительное или отрицательное состояния событий, поэтому не рекомендуется внедрять 100%-ный уровень автоматизации. Также компоненты когнитивной системы могут быть подвержены атакам, целью которых является манипулирование данными, что в конечном итоге создает бреши в системе обеспечения безопасности. Внедряемая модель когнитивной безопасности должна учитывать вышеупомянутый недостаток и включать в себя методы контроля, такой как, например, MAPE-K (Monitor-Analyze-Plan-Execute over a shared Knowledge). При этом немаловажно сохранение аналитика как части модели с помощью OODA и HITL (Human-in-the-loop), а также формирование многоуровневой модели, которая позволяет анализировать качество данных.

Осведомленность о ситуации в области кибербезопасности позволяет организациям оценить свое текущее состояние, оценить уязвимости, предупредить атаки и просчеты. На основе этих знаний организации могут прогнозировать свои состояния в ближайшем будущем. И существует два возможных уровня осведомленности о ситуации в области кибербезопасности:

- низкий уровень, на котором обрабатываются первичные данные, которые наиболее часто используются для поиска технологических решений, позволяющих их автоматизировать;
- высокий уровень, позволяющий принимать стратегические решения на основе методов абстракции. Высокий уровень ситуационной осведомленности обычно выполняется людьми вручную, это трудоемко, отнимает много времени и чревато ошибками.

Когнитивная модель безопасности рассматривает различные источники информации для установления осведомленности о ситуации:

1. HUMINT, генерируется людьми из интервью, бесед или форумов.
2. SIGINT, создается путем перехвата сигналов, генерируемых компьютерным оборудованием, сетевым оборудованием или телекоммуникационным оборудованием.
3. OSINT, получен из открытых источников и включает новости, социальные сети и коммерческие базы данных. В нем также рассматривается техническая информация с таких платформ, как WHOIS.
4. MASINT, создается на основе данных, полученных от измерительных приборов. Датчики могут использоваться тактически или стратегически для получения такого рода информации.
5. GEOINT, создается из геопространственных систем и может быть полностью получен из любых спутниковых или аэрофотоснимков.

Объем информации может превышать аналитические возможности специалистов по безопасности, в следствие чего встает необходимость использования Рекомендательных систем (RS) или Экспертных систем поддержки принятия решений (DSS).

Наиболее отвечающей задачам безопасности может быть модель, состоящая из следующих семи уровней, которые объединяют различные технологические решения и улучшают когнитивные навыки аналитика безопасности [11].

1. Уровень источника информации. На этом уровне рассматриваются различные источники данных, генерируемые серверами, сетевым оборудованием, оборудованием для обеспечения безопасности и пользовательскими устройствами.
2. Уровень датчиков. Этот уровень обеспечивает однородность сообщений датчиков безопасности, распределенных между несколькими точками.
3. Уровень сбора. На этом уровне выполняется процесс управления данными. Процесс управления данными включает в себя: проверку данных, очистку данных, преобразование данных, а также разделение данных.
4. Уровень предварительной обработки. На этом уровне устанавливаются шаблоны аномального поведения, на основе которых можно определить наличие возможных атак. Шаблоны устанавливаются на основе корреляции данных сетевого трафика, поведения пользователя, установленных подключений и используемых сетевых адресов.
5. Уровень моделирования. На этом уровне необходимо выполнить моделирование собранной информации, описать потоки данных и установить наиболее распространенные типы взаимодействия, которые существуют внутри сети.
6. Уровень обработки. Этот уровень также использует решения машинного обучения с целью анализа аномального поведения или параметров на уровне визуализации. На этом уровне визуализация информации, генерируемой уровнем обработки, представлена в виде источников, которые

не повреждены и не изменены.

7. Уровень принятия решений. На этом уровне представлена визуализация информации, генерируемой уровнем обработки. Можно использовать системы рекомендаций или Системы поддержки принятия решений.

В таблице приводится исследование когнитивных технологии в части их применения в цепочке модели обеспечения кибербезопасности.

Использование цикла OODA определяет шаблоны, которые выявляются путем анализа данных для генерации ментальных моделей в базе профилей атак, угроз, поведения пользователей и атакующих, которые позволяют установить осведомленность организации о ситуации и определить действия для поддержания необходимого состояния кибербезопасности [10]. OODA делится обработанной информацией с аналитиком безопасности через системы рекомендаций или системы поддержки принятия решений.

Непрерывный мониторинг состояния кибербезопасности может быть достигнуть путем применения циклов MAPE-K, являющейся наиболее влиятельной эталонной моделью управления для автономных и самоадаптивных систем.

Включение человеческого фактора в модель когнитивной безопасности может быть обеспечено благодаря модели HITL. Данная ветвь искусственного интеллекта связана с интеграцией как человеческого, так и машинного интеллекта для создания моделей машинного обучения. Специалисты тренируют, настраивают и тестируют определенные алгоритмы для будущего автономного решения прогнозируемых проблем и задач. HITL позволяет контролировать генерацию ложных предупреждений, на основе чего осуществляет управление исполнительными механизмами реагирования и автоматически избегает действий, которые могут негативно повлиять на систему, особенно когда они являются результатом ложных предупреждений.

Но глобально, говоря в целом о применении информационных технологий в области кибербезопасности, традиционно подразумевается машинное обучение (ML), в которой входными данными классификатора угроз являются экспертные решения, а сама классификация угроз является результатом. В качестве же когнитивной технологии, а не метода оптимизации, применяется методология глубокого обучения (DL), специфика которой позволяет работать с большими и неотсортированными данными. Последний факт выгодно различает DL от ML, однако проблема данной методологии заключается в том, что на этапе обучения она требует тысячи или миллионы примеров, в то время как имеющиеся входные экспертные решения, как правило, исчисляются десятками или сотнями. Более того, подходы DL в значительной степени необъяснимы, то есть у аналитика нет возможности узнать причину того, почему было выделено конкретное предупреждение. В качестве альтернативы выдвигается символическое глубокое обучение (SDL). Во-первых, этот метод способен создавать классификаторы из небольшого числа примеров, как ML. Во-вторых, в то время как DL создает модель поведения «черного ящика», SDL создает объяснимую модель экспертного познания — расширяемую иерархическую сеть памяти, основанную на экспертном опыте и решениях.

Наглядно сравнить специфику методологий DL и SDL можно, оценив результаты, достигаемые ими в равных условиях в ходе эксперимента. Эксперимент, о котором далее будет идти речь,

Когнитивные технологии в разрезе уровней модели обеспечения кибербезопасности

Сфера	Уровень	Область применения	Методология
Когнитивные технологии	Предварительная обработка	Самоадоптация	MAPE-K
		Ситуативная осведомленность	OODA
	Моделирование	Модель угроз	Cognitive maps
		Модель атак	Game theory
		Модель планирования	Fuzzing
		Модель рисков, Модель влияния	Ontologies
	Обработка	Системы поддержки принятия решений	Intelligence driven
			Data driven
		Рекомендательные системы	User driven Goal driven
	Визуализация	Безопасность, визуализация	Geo-maps
			Traffic flow
		Big Data Analytics	Time series
			Correlation graphs
			Forensic events

Источник: составлено автором по [5—7; 10]

был разработан как часть исследования способности человека оценивать киберугрозы, подобно IDS[1], на основе небольшого набора инструкций [12]. В этом эксперименте участникам были представлены четыре пакета записей о кибератаках, где в пакете 1 было 40 записей, в пакете 2 было 60 записей, в пакете 3 было 80 записей, а в пакете 4 было 100 записей. Каждая запись состояла из четырех признаков, относящихся к обнаруженной сетевой активности: отметка времени, номер порта источника, страна и описание предупреждения (например, “FTP — Подозрительная команда MGET”, “ET TROJAN Qhosts Trojan Checkin”). Для каждой такой записи участники могли нажать либо переключатель «Угроза», либо переключатель «Нет угрозы». Половина записей в каждой партии содержала угрозы. Участникам не была предоставлена обратная связь относительно того, были ли их классификации угроз правильными. Это исследование было проведено онлайн с использованием Amazon Mechanical Turk, и был задействован шестьдесят один участник.

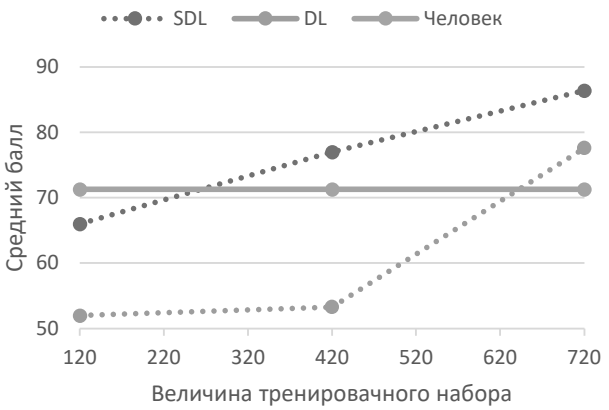
Пакеты 1, 2 и 3 были использованы в качестве данных для обучения моделей, а пакет 4 (содержащий 100 случаев записи) был проверочным. Самый высокий общий балл идентификации для партий 1, 2 и 3 составил 0,883, и этот балл был достигнут четырьмя участниками. Этих четырех участников классифицировали как «экспертов», и на основе их решений обучались модели SDL и DL.

Средний общий балл в 4-й партии для участников, не являющихся экспертами, составил 71,3%, при этом средний показатель попадания (правильно идентифицированные угрозы) составил 0,725, а частота ложных срабатываний — 0,2984. В этом эксперименте чувствительность для неэксперта в партии 4 составила d’ = 1,128 (более высокий d’ предполагает более высокую чувствительность).

Модель SDL, обученная 5 на экспертных решениях из партий 1, 2 и 3 (180 случаев × 4 эксперта), дала средний балл 86,4% в партии 4, со средним показателем попадания 0,796 и средним показателем ложной тревоги 0,069, d’ = 2,31.

Модель DL, обученная 6 на экспертных решениях из партий 1, 2 и 3, дала средний балл 77,6% в партии 4, со средним показателем попадания 0,701 и средним показателем ложных тревог 0,149, d’ = 1,57.

На рисунке показаны общие показатели производительности для SDL и DL с учетом трех размеров тренировочных наборов.



Средний правильный классификационный балл для моделей SDL и DL в пакете 4

Источник: составлено автором по [12].

Один из наиболее очевидных выводов заключается в том, что SDL работает намного лучше с меньшими наборами данных, чем традиционные методы DL. Это имеет большое значение в области кибербезопасности, где трудно получить экспертные данные. Возможно, не следует удивляться тому, что методология когнитивного моделирования более подходит для создания вспомогательных средств принятия решений на основе небольших выборок индивидуальных решений, чем методы искусственного интеллекта, предназначенные для математической оптимизации больших объемов данных. К сожалению, из-за популярности традиционной методологии ML когнитивные вычисления часто не принимаются во внимание, даже когда они могут быть подходящим инструментом для работы. Что еще более важно, отбор опытных исполнителей в реальном мире имеет первостепенное значение для получения аналогичных данных обучения. Один из вопросов, который может прийти на ум, заключается в том, нужны ли люди вообще. Если это так, что производительность SDL составляет 86,4 %, в то время как ожидается, что производительность человека, не являющегося экспертом, составит от 71,3. Однако этот сценарий предполагает статичную работу неспециалиста, в то время как люди учатся и адаптируются. Новички могут начинать с более низкого уровня производительности, но при наличии экспертной обратной связи их производительность улучшается. Поддержка принятия решений на основе когнитивного моделирования предназначена не для того, чтобы вытеснить неспециалистов, а скорее для того, чтобы дать им оперативную экспертную обратную связь, чтобы помочь им принимать лучшие решения на ранних этапах испытаний и достигать результатов на уровне экспертов быстрее, чем это произошло бы в противном случае.

[1] Intrusion Detection System (англ. Система обнаружения вторжений).

Комплекс же проблем, связанных с внедрением когнитивных технологий в модели кибербезопасности, представлен следующим образом.

Первая проблема или вызов, с которыми сталкивается когнитивная безопасность, заключается в том, что для прогностического анализа источники данных не должны быть изменены или повреждены, для чего необходимо установить процессы обеспечения качества данных и механизмы безопасности, которые позволяют избежать изменения источников данных. Если злоумышленник изменит данные, это может привести к анализу, машинному обучению и последующим решениям, базирующихся на ложных данных, что в конечном итоге побудит аналитика принять неверное решение.

Вторая проблема заключается в ограниченности когнитивных технологий, что в отличие от человека еще не обладают автономным здравым смыслом для решения дилемм [5].

Наконец, третья проблема заключается в том, что когнитивным технологиям все еще не хватает способности к обобщению и абстракции, которые позволяют людям решать проблемы и анализировать возможные последствия принятых решений. Исходя из этого критерия, не каждый процесс можно автоматизировать из-за риска наличия ложных срабатываний. В случае полной автоматизации ложное срабатывание может привести к критическим ошибкам системы, поэтому необходимо включать в такие модели HITL.

В заключение необходимо сказать, что использование когнитивных наук в области кибербезопасности позволяет учитывать вклад психологии, искусственного интеллекта, лингвистики и взаимодействия человека и компьютера для улучшения когнитивных процессов аналитиков безопасности, сокращать время реагирования и повышать эффективность при принятии решений о действиях по обнаружению, сдерживанию или смягчению угрозы безопасности.

Список литературы

1. Abdelwahed, S., Model-based response planning strategies for auto- nomic intrusion protection / S. Abdelwahed, S. Iannucci // ACM Trans Auton Adapt Syst. 2018. Vol. 13. P. 23—35.

2. Amara, N. Cloud computing security threats and attacks with their mitigation techniques / N. Amara, H. Zhiqui, A. Ali // International conference on cyber-enabled distributed computing and knowledge discovery (CyberC). 2020. P. 53—67.

3. Andrade, R. Management of information security indica- tors under a cognitive security model / R. Andrade, J. Torres, P. Flores // 8th Annual Computing and Communication Workshop and Conference (CCWC). 2018. P. 478—483.

4. Latrache, A. Multiagent based incident management system according to ITIL / A. Latrache, H. Nfaoui, J. Boumhidi // Intelligent systems and computer vision (ISCV). 2015. Vol. 10. Pp. 1—7.

5. Security issues in the internet of things (IoT): a comprehensive study / A. Mirza, Muhammad, H. Sajid, U. Saleem // International Journal of Advanced Computer Science and Applications. 2017. Vol. 8 (6). Pp. 153—168.

6. Maglaras, L. Cybersecurity in the Era of Digital Transformation / L. Maglaras, G. Drivas // Proceedings of the 2020 International Conference on Internet of Things and Intelligent Applications (ITIA). 2020. Pp. 1—5.

7. Software platforms for smart cities: concepts, requirements, challenges, and a unified reference architecture / E. Santana, A. Chaves, M. Gerosa, F. Kon, D. Milojicic // ACM Computing Surveys. 2021. Vol. 78. Pp. 345—347.

8. Scott, J.Intelligence driven incident response / J. Scott, B. Rebekah. 1st edition California : O'Reilly Media, Inc, 2017. Pp. 437.

9. Shameli-Sendi, L. H. Dynamic optimal countermeasure selection for intrusion response system / L. H. Shameli-Sendi, M. Cheriet // IEEE Transactions on Dependable and Secure Computing. 2018. Vol. 12. Pp. 34—37.

10. SonicWall Cyber Threat Report 2022: Mid-Year Update // SonicWall. 2022. Pp. 14.

11. Thomas W.,Research methods for cybersecurity / W. Thomas, D. Manz. 1st edition. California : Syngress, 2017. Pp. 352.

12. Veksler D., Buchler N. Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior / D. Veksler, N. Buchler // Cognition journal. Vol. 34. 2020. Pp. 12—35.

Сведения об авторах

Сулейманова Данна Олхазеровна — магистрант кафедры «Информационные системы в экономике» Грозненского государственного нефтяного технического университета им. акад. М. Д. Миллионщикова. *dana.s.o.00s3@gmail.com*.

Магомаев Тамирлан Рамзанович — старший преподаватель кафедры «Информационные системы в экономике» Грозненского государственного нефтяного технического университета им. акад. М. Д. Миллионщикова. *prikl-inf@mail.ru*.