НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

DOI 10.35264/1996-2274-2020-1-169-177

НАУЧНО-ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ РАЗВИТИЯ ТЕХНОЛОГИЙ КИБЕРБЕЗОПАСНОСТИ ЗА РУБЕЖОМ

Д.Б. Изюмов, нач. отд. ФГБНУ НИИ РИНКЦЭ, *izyumov@extech.ru*
Е.Л. Кондратюк, зам. нач. отд. ФГБНУ НИИ РИНКЦЭ, *kel@extech.ru*
Рецензент: С.В. Стрельников

В статье рассмотрены понятие кибербезопасности и ее особенности, представлены перечень регламентирующих документов США в области киберпространства и кибербезопасности, а также значимые научно-исследовательские и опытно-конструкторские работы и программы в области развития технологий кибербезопасности, проводимые Управлением перспективных исследовательских проектов Минобороны США (DARPA). Обобщены наиболее распространенные зарубежные технологии, используемые для защиты компьютеров, интеллектуальных устройств, маршрутизаторов, сетей и облачных сред, а также основные научно-технические проблемы развития технологий кибербезопасности.

Ключевые слова: кибербезопасность, киберпространство, кибератака, киберугроза, технология, информационно-коммуникационная система, машинное обучение, искусственный интеллект, программно-аппаратное средство, информационно-управляющая система, блокчейн, биометрическая аутентификация, стратегия.

SCIENTIFIC AND TECHNOLOGICAL PROBLEMS OF THE DEVELOPMENT OF CYBERSECURITY TECHNOLOGIES ABROAD

D.B. Izyumov, Head of Department, SRI FRCEC, *izyumov@extech.ru*
E.L. Kondratyuk, Deputy Head of Department, SRI FRCEC, *kel@extech.ru*

The article discusses the concept of cybersecurity and its features, presents a list of US regulatory documents in the field of cyberspace and cybersecurity, as well as significant research and development work and programs in the field of development of cybersecurity technologies conducted by the Department of Advanced Research Projects of the US Department of Defense (DARPA). The most common foreign technologies used to protect computers, smart devices, routers, networks and cloud environments, as well as the main scientific and technological problems of the development of cybersecurity technologies, are summarized.

Keywords: cybersecurity, cyberspace, cyberattack, cyberthreat, technology, information and communication system, machine learning, artificial intelligence, software and hardware, information management system, blockchain, biometric authentication, strategy.

В настоящее время за рубежом, особенно в США, развитию мер и технологий кибербезопасности уделяется самое пристальное внимание. Под кибербезопасностью понимается реализация комплекса мер по обеспечению многоуровневой защиты информационно-коммуникационных систем, компьютеров, сетей, программ и программных приложений, баз

и хранилищ данных от умышленных и случайных цифровых атак (кибератак), которые обычно направлены на получение доступа к конфиденциальной информации, ее изменение (искажение) и/или уничтожение, блокирование, кражу, а также на нарушение нормального функционирования министерств, ведомств, центров, лабораторий, компаний и предприятий[1].

При этом под защитой данных следует понимать обеспечение конфиденциальности, доступности, целостности и аутентичности информации. На сегодняшний день выполнять все эти функции одновременно не может ни одна из технологий кибербезопасности, поэтому соблюдение каждого из перечисленных принципов требует использования соответствующих решений.

Многоуровневая защита достигается объединением (дополнением) сотрудников, рабочих процессов и технологий кибербезопасности в единую организационную систему. Так, например, к настоящему времени самым большим источником риска в области кибербезопасности остается человеческий фактор, – по опросам зарубежных специалистов, 34 % успешных кибератак (киберинцидентов) связаны с ошибками, беспечностью, неосмотрительностью и непреднамеренными действиями сотрудников (персонала организации), еще 26 % – с устаревшими средствами контроля и безопасности в области IT-технологий, 13 % – с возможностью несанкционированного доступа, 10 % – с использованием облачных сервисов. Оставшиеся 17 % связаны с иными причинами, включая намеренное причинение физического вреда (саботаж) собственными сотрудниками организаций и извне, ошибки в программном обеспечении, отказ аппаратного обеспечения и др. [1]

Среди ведущих зарубежных стран (ВЗС) наибольшее внимание вопросам и проблемам выстраивания эффективной системы кибербезопасности, а также развития соответствующих технологий уделяется в США, которые занимают первое место на мировом технологическом рынке обеспечения функционала кибербезопасности. К настоящему времени США контролируют 16 % мирового рынка технологического обеспечения информационной безопасности, второе место с долей 5 % занимает Израиль.

По мнению американского военно-политического руководства, необходимость принятия мер по нейтрализации угроз национальной безопасности в киберпространстве обусловлена прежде всего стремительным ростом зависимости государственных и коммерческих структур от использования различных автоматизированных информационно-управляющих систем (ИУС), а также высоким уровнем их уязвимости[2]. Значительная роль при этом отводится Министерству обороны (МО) США, которое финансирует многочисленные научно-исследовательские и опытно-конструкторские работы (НИОКР), направленные на совершенствование и разработку полного спектра средств (оборонительных, разведывательных и наступательных), необходимых для сдерживания вероятного противника в киберпространстве. Так, в США в целях эффективного реагирования вооруженных сил (ВС) на угрозы национальной безопасности в киберпространстве в 2010 г. было сформировано командование боевых действий в кибернетическом пространстве (United States Cyber Command – USCYBERCOM), которое в масштабах ВС страны является главным органом управления боевыми действиями в этой сфере и отвечает за решение комплекса профильных задач (рис. 1). А уже с 2011 г. в США за киберпространством закреплен статус одной из ключевых сфер ведения боевых действий наряду с традиционными (воздушно-космическая, наземная

[1] Здесь и далее подразумеваются министерства, ведомства и различные организации сектора военно-промышленного комплекса (ВПК) ведущих стран мира.

[2] По оценке американских экспертов, в настоящее время ежечасно выявляется не менее 250 тыс. попыток несанкционированного доступа в компьютерные сети Пентагона, при этом в целом на правительственные и ведомственные информационные ресурсы США ежемесячно совершается около 2 млрд кибератак различной сложности и направленности.

и морская). В последующие годы были приняты две важнейшие стратегии в области киберпространства и кибербезопасности:

– в 2015 г. – Стратегия действий Министерства обороны США в киберпространстве (Department of Defense Cyber Strategy);

– в 2018 г. – Национальная киберстратегия (National Cyber Strategy).

Рис. 1. Киберкомандование ВС США

Эти документы полностью согласованы с обновленной в 2018 г. Стратегией национальной безопасности США (National Security Strategy), определяют основные направления развития киберпотенциала ВС страны, предъявляемые к нему требования, взгляды американской администрации на вызовы и угрозы в цифровой сфере, обеспечение информационной безопасности и организацию сдерживания противника в компьютерных сетях, всестороннюю защиту интересов страны, а также порядок решения общенациональных и ведомственных задач в киберпространстве [1, 2].

Однако, в соответствии с аналитическим докладом Научного комитета МО США, несмотря на осуществленные за последнее десятилетие значительные организационно-структурные преобразования и законодательные усилия, существующие технологии кибербезопасности и возможности не обеспечивают надежную защиту киберпространства от атак, проводимых с использованием неизвестных ранее инновационных технологических решений.

По оценкам американских специалистов в области информационной безопасности, наиболее вероятными источниками угроз для ИУС являются спецслужбы иностранных государств, террористические и преступные группировки, промышленно-финансовые группы, хакеры, а также лица, допущенные к работе с системами в порядке служебной деятельности (инсайдеры). По заявлению заместителя министра обороны США, более 100 иностранных разведок за последние годы пытались проникнуть в военные компьютерные сети США. Стоит подчеркнуть, что только по открытым программам МО США на обеспечение и совершенствование системы военной кибербезопасности ежегодно выделяется 1,5–3,0 млрд долл., из которых около 500 млн долл. направлены на исследования в области новых кибертехнологий с акцентом на оборонительный аспект [3].

К значимым НИОКР и программам в области развития технологий кибербезопасности стоит отнести следующие работы, проводимые Управлением перспективных исследовательских проектов МО США (DARPA):

– НИОКР «Интегрированные системы безопасности аппаратно-программных средств» (Cyber Fault-Tolerant Attack Recovery), направленная на повышение устойчивости средств обработки информации за счет криптографических вычислений и верификации аппаратного обеспечения;

– НИОКР «Устойчивые к кибератакам системы восстановления работоспособности инженерных ресурсов» (Systems Security Integrated Through Hardware and Software), направленная на снижение вероятности несанкционированного доступа к ресурсам военных и правительственных сетей;

– НИОКР «Активная кибероборона» (Active Cyber Defense), направленная на разработку специализированных программно-технических средств в области кибербезопасности;

– НИОКР «Комплексные кибероперации» (Symbiotic Cyber Operations), направленная на развитие средств и способов ведения наступательных и оборонительных действий в киберпространстве, оценку и выявление уязвимостей систем защиты информации вероятного противника;

– НИОКР «Конфигурация безопасности» (Configuration Security), направленная на исследование адаптивных систем защиты информации, методов и способов обнаружения и устранения уязвимостей информационных систем, интегрированных в объекты критической инфраструктуры и военную технику США;

– НИОКР «Защита от крупномасштабных скоординированных атак «отказ в обслуживании» (Extreme Distributed Denial of Service Defense), направленная на разработку новых архитектурных решений построения сетей, внедрение в глобальном масштабе устройств сканирования и фильтрации трафика с элементами машинного обучения, а также на имитацию ложной деятельности в информационно-коммуникационных сетях;

– программа «План Икс» (Plan X), направленная на повышение эффективности взаимодействия операторов с киберпространством, создание технологии автоматизированного анализа и трехмерной визуализации телекоммуникационных сетей, программно-технических средств планирования действий в киберпространстве, оценки вероятного ущерба от кибератак, а также на подготовку специалистов по проведению кибероперации;

– программа «Радикс» (RADICS), направленная на разработку средств защиты сетевой и вычислительной инфраструктуры объектов американской электроэнергетики от кибервоздействий, а также на разработку единых стандартов по разделению аппаратных, сетевых и информационных ресурсов на национальные, союзные и иные;

– программа «Сетевая защита» (Network Defense), направленная на вовлечение национальных корпораций в процесс обеспечения государственной безопасности и переход от локальной защиты информации к совместной путем создания системы распознавания подозрительного поведения пользователей сети Интернет и пресечения их незаконной деятельности в киберпространстве;

– другие программы, преимущественно нацеленные на повышение точности и оперативности ведения киберразведки, совершенствование методов изучения состава и поведения участников информационного обмена в киберпространстве, на автоматизацию процесса установления подлинности сообщений, видеофрагментов и изображений в информационных сетях и т. п.

За последние три года объем финансирования DARPA работ в области кибербезопасности вырос на 16 %: с 331,7 млн долл. в 2016 г. до 395,3 млн долл. в 2019 г. [4].

Анализ проводимых исследований и разработок показывает, что технологии кибербезопасности являются важнейшим элементом, предоставляющим организациям и отдельным пользователям инструменты, необходимые для защиты от кибератак. В целом за рубежом

к наиболее распространенным технологиям, используемым для защиты компьютеров, интеллектуальных устройств, маршрутизаторов, сетей и облачных сред, относятся:

– межсетевые экраны нового поколения;

– шлюзы антивирусной защиты (антивирусное программное обеспечение) и фильтрации контента (фильтрация DNS)[3];

– защита от вредоносного программного обеспечения (ПО);

– блокчейн[4];

– искусственный интеллект (ИИ) и технология машинного (глубокого) обучения;

– биометрическая аутентификация;

– криптографическое шифрование информации;

– различные решения для защиты электронной почты и др. [5].

Так, внедрение и использование возможностей ИИ и технологии машинного обучения позволяет обнаруживать и устранять бóльшую часть кибератак, цель которых – вывод из строя сайтов компаний, компрометация конфиденциальных данных и их хищение, включая хищение денежных средств организаций. В частности, решения, основанные на технологиях ИИ и машинного обучения, позволяют предотвращать кибератаки, направленные на датчики и контроллеры, установленные на объектах промышленного производства сектора ВПК. В данном случае ИИ анализирует все изменения в производственных процессах и информирует специалистов предприятия о потенциальных атаках. Более того, система обнаружения кибератак, построенная по технологии машинного обучения, способна моментально информировать персонал (сотрудников организации) о переходе по подозрительным ссылкам, присылать сообщения об отправке нежелательного ответа получателям за пределами домена, а также предлагать различные встроенные функции защиты от новых киберугроз.

Стоит подчеркнуть, что аналитика в кибербезопасности, а также облачные и мобильные технологии являются наиболее приоритетными зарубежными технологиями в области информационной безопасности [6,7].

Анализ текущих и долгосрочных планов развития, обновления и модернизации системы информационной безопасности США, Национальной киберстратегии страны, а также открытых программ Министерства обороны (включая программы и проекты DARPA) на обеспечение и совершенствование системы военной кибербезопасности показал, что основными научно-техническими проблемами развития технологий кибербезопасности являются:

– разработка и развитие оперативных концепций обеспечения безопасности военных компьютерных сетей и систем, а также архитектур их построения (например, внедрение в глобальном масштабе устройств сканирования и фильтрации трафика с элементами машинного обучения);

– качественное усовершенствование компьютерной и сетевой архитектуры;

– создание общего информационного пространства и единой системы кибербезопасности;

– развитие и разработка новых надежных операционных систем, нового программного обеспечения и соответствующих приложений в области информационной безопасности;

---

[3] DNS-фильтрация – это высокоскоростная фильтрация трафика в сети Интернет без ограничений по объему и полосе пропускания трафика; контент-фильтр DNS позволяет пользователям управлять доступом к онлайн-ресурсам, избавляет от ненужной и вредной информации в Сети.

[4] Блокчейн представляет собой технологию цепочек взаимосвязанных информационных блоков, хранимых и разнесенных на разных компьютерах (распределенная база данных). Технология блокчейна ориентирована больше на защиту финансовых ресурсов организаций (финансового сектора), может применяться при идентификации пользователей сети и создании различных приложений в области кибербезопасности. Технология блокчейна гарантирует не только сохранность, но и неизменность и подлинность данных, а также делает практически невозможным взлом систем идентификации.

– проведение сбора и анализа сведений об угрозах: URL-адресах, доменах, IP-адресах, контрольных суммах файлов, названиях угроз, статистики и поведенческих данных, данных WHOIS/DNS и т. п.;

– разработка специальных программно-аппаратных средств (например, средств обнаружения кибератак и вторжений);

– повышение уровня индивидуальной защиты автоматизированных информационно-управляющих систем (прежде всего – за счет поддержания в рабочем состоянии и своевременного обновления специального защитного программного обеспечения и операционной системы, а также использования лучших коммерческих разработок в области обеспечения компьютерной, сетевой и информационной безопасности);

– создание и развертывание новых автоматизированных систем и сетей передачи данных в целях многократного резервирования существующих автоматизированных информационно-управляющих систем;

– повышение точности и оперативности определения конкретных источников деструктивных действий в киберпространстве;

– обеспечение встраивания алгоритмов киберзащиты на этапе проектирования информационно-коммуникационных систем;

– повышение приоритетности поэтапной разработки, тестирования и внедрения сложной системы перед ее комплексной сдачей в эксплуатацию;

– создание и развитие целостной многоуровневой системы управления киберрисками;

– усиление и развитие мер активной защиты, направленных на обнаружение, анализ и подавление киберугроз и уязвимостей в режиме реального времени с применением специальных аппаратно-программных средств;

– совершенствование системы автоматизированного обмена информацией;

– разработка и развитие технологий доступа к нужным сетям при отсутствии подключения к сети Интернет;

– разработка интеллектуальных сетевых экранов нового поколения;

– развитие технологий поведенческого анализа (User and Entity Behavior Analytics – UEBA);

– развитие методов и способов биометрической аутентификации (подразумевается использование «закрытых данных», таких как сердечный пульс человека, форма мочек ушей, рисунок внутриглазных сосудов, а также имплантирование под кожу чипов, анализ нейронных связей человека, тест ДНК, использование таблеток-компьютеров и др.);

– обеспечение гарантированного исключения принятия искусственным интеллектом (суперкомпьютером) неверных решений (так, специалисты по кибербезопасности до сих пор не смогли полностью решить проблему защиты от «ложных срабатываний» при использовании искусственного интеллекта; данное направление имеет важнейшее значение для развития информационной безопасности в будущем);

– развитие технологии машинного (глубокого) обучения;

– повышение устойчивости средств обработки информации за счет криптографических вычислений и верификации аппаратного обеспечения;

– внедрение и развитие технологии квантовой криптографии[5];

[5] Квантовая криптография – это технология, позволяющая обеспечить практически абсолютную защиту шифрованных данных от взлома, основанная на принципе квантового распределения ключей в квантовой сети. При попытке взлома такой сети фотоны, передающие информацию, меняют свое состояние, внося ошибки в передаваемые данные. К настоящему времени эта технология пока не используется на практике, однако уже близка к этому. За рубежом активные исследования в этой области проводят компании IBM, GAP-Optique, Mitsubishi, Toshiba, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт, а также холдинг QinetiQ, поддерживаемый британским Министерством обороны. Считается, что данное направление позволит существенно улучшить методы защиты переноса данных.

– внедрение и развитие технологии защиты движущейся цели[6];

– разработка технологии обнаружения «инфицированных» процессоров ЭВМ, параллельно выполняющих одинаковую задачу (цель – снижение вероятности несанкционированного доступа к ресурсам военных и правительственных сетей);

– ускорение процесса приобретения новых информационных и технологий кибербезопасности (например, за счет отказа или переноса сроков некоторых заказов в пользу быстрых пошаговых улучшений уже разработанных систем; сокращения времени проведения профильных НИОКР с 7–8 до 1–3 лет; проведения многоуровневой проверки на всех этапах модернизации как специального, так и общего программного обеспечения; ужесточения мер безопасности для всех систем, закупаемых Министерством обороны, включая программное обеспечение и аппаратное оборудование, и других мер);

– разработка и создание электронной компонентной базы (процессоров, микросхем, чипов памяти и других комплектующих) собственного производства (данное направление имеет комплексный характер: от защиты собственных информационно-управляющих систем от так называемых «закладок» до развития национальной отрасли и технологий производства электронной компонентной базы в целом);

– разработка единых стандартов обеспечения кибербезопасности и их внедрение в автоматизированные системы органов государственной власти, частных корпораций и сети общего пользования как в США, так и в странах-партнерах;

– разработка специализированных программно-технических комплексов для отработки мероприятий оперативной и боевой подготовки ВС США, связанных с кибербезопасностью;

– создание технологии автоматизированного анализа и трехмерной визуализации телекоммуникационных сетей;

– развитие партнерских отношений с союзниками по блоку НАТО и другими международными партнерами для укрепления коллективной кибербезопасности (это целый блок проблем, направленный на разработку новых возможностей, технологий и поддержание коллективных усилий по кибербезопасности; усиление мер защиты секретной информации сектора ВПК; выработку единого комплекса правительственных и межправительственных мер, направленных на управление рисками, связанными с импортом информационных и телекоммуникационных технологий, увеличением количества контрафактных программных продуктов и аппаратных компонентов; развитие системы международного обмена информацией, включая своевременные сообщения о кибернетической деятельности и инцидентах, о сигнатурах (ключах) выявленных вредоносных программных кодов, о враждебных лицах и группировках);

– разработка новых методик и концепций обучения персонала, ужесточение мер отчетности, внутреннего мониторинга и управления информационными потоками, а также индивидуальной ответственности за нарушение требований безопасности;

– выработка, создание и совершенствование условий для привлечения высококвалифицированных специалистов в области кибербезопасности из гражданских и коммерческих структур [8, 9].

Таким образом, анализ научно-технических проблем развития технологий кибербезопасности в ведущих зарубежных странах показал, что к настоящему времени среди приоритетных зарубежных технологий информационной безопасности стоит выделить аналитику

[6] В основе технологии защиты движущейся цели лежит принцип исключения доступа авторов кибератак к коду, который используется при шифровании данных. По мнению ряда зарубежных экспертов, в настоящее время наличия одного факта шифрования информации недостаточно. Для надежной защиты данных необходимо непрерывно изменять систему. Данная технология также является новой в сфере кибербезопасности (впервые была представлена в США в 2016 г.) и пока широкого распространения не получила.

в кибербезопасности, облачные и мобильные технологии. К менее приоритетным технологиям кибербезопасности в ВЗС относят искусственный интеллект, блокчейн и биометрическую аутентификацию. При этом, несмотря на некоторые недавно появившиеся технологии кибербезопасности, большинство существующих технологий были представлены более десяти лет назад, включая технологии машинного обучения и технологии детектирования в облаке.

По мнению зарубежных специалистов, в среднесрочной и долгосрочной перспективе наибольшее применение и развитие получат решения, предназначенные для предупреждающего выявления кибератак и нарушений систем информационной безопасности.

Основные научно-технические проблемы в рассматриваемой области связаны с уровнем технической и технологической оснащенности ведущих развитых зарубежных стран, их возможностей в сфере информационно-телекоммуникационных и компьютерных технологий, а также с наличием высококвалифицированных IT-специалистов и специалистов в области кибербезопасности.

Статья выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках государственного задания 2020 г. № 075-01394-20-02.

Список литературы

1. National Cyber Strategy of the United States of America. September 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 13.04.2020).

2. Department of Defense Cyber Strategy. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_ SUMMARY_FINAL.PDF (дата обращения: 13.04.2020).

3. TechBeacon: 5 emerging security technologies set to level the battlefield. URL: https://techbeacon.com/security/5-emerging-security-technologies-set-level-battlefield (дата обращения: 13.04.2020).

4. Information Age: 10 cyber security trends to look out for in 2019. URL: https://www.information-age.com/10-cyber-security-trends-look-2019-123463680.

5. SRI International: Cyber Security Research & Development Center. URL: https://www.sri.com/work/projects/csrdc (дата обращения: 13.04.2020).

6. IBM: Cyber Security Technologies. URL: http://www.research.ibm.com/haifa/dept/vst/csqt.shtml (дата обращения: 13.04.2020).

7. CyberDegrees: Hot Technologies in Cyber Security. URL: https://www.cyberdegrees.org/resources/hot-technologies-cyber-security (дата обращения: 13.04.2020).

8. Lauren C. Williams. DARPA takes on cyber defense with hackathons. Mar 08, 2019. URL: https://fcw.com/articles/2019/03/08/darpa-chase-cyber-williams.aspx (дата обращения: 13.04.2020).

9. DARPA Prototypes New AI-Enabled «Breakthrough» Cyberattack «Hunting» Technology. URL: https://defensemaven.io/warriormaven/cyber/darpa-prototypes-new-ai-enabled-breakthrough-cyberattack-hunting-technology-6yKXpdVGuUupUV-xgIJ9cA (дата обращения: 13.04.2020).

References

1. National Cyber Strategy of the United States of America. September 2018. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed: 13.04.2020).

2. Department of Defense Cyber Strategy. Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed: 13.04.2020).

3. TechBeacon: 5 emerging security technologies set to level the battlefield. Available at: https://techbeacon.com/security/5-emerging-security-technologies-set-level-battlefield (accessed: 13.04.2020).

4. Information Age: 10 cyber security trends to look out for in 2019. Available at: https://www.information-age.com/10-cyber-security-trends-look-2019-123463680 (accessed: 13.04.2020).

5. SRI International: Cyber Security Research & Development Center. Available at: https://www.sri.com/work/projects/csrdc (accessed: 13.04.2020).

6. IBM: Cyber Security Technologies. Available at: http://www.research.ibm.com/haifa/dept/vst/csqt.shtml (accessed: 13.04.2020).

7. CyberDegrees: Hot Technologies in Cyber Security. Available at: https://www.cyberdegrees.org/resources/hot-technologies-cyber-security (accessed: 13.04.2020).

8. Lauren C. Williams. (2109) DARPA takes on cyber defense with hackathons. Mart 08. Available at: https://fcw.com/articles/2019/03/08/darpa-chase-cyber-williams.aspx (accessed: 13.04.2020).

9. DARPA Prototypes New AI-Enabled «Breakthrough» Cyberattack «Hunting» Technology. Available at: https://defensemaven.io/warriormaven/cyber/darpa-prototypes-new-ai-enabled-breakthrough-cyberattack-hunting-technology-6yKXpdVGuUupUV-xgIJ9cA (accessed: 13.04.2020).