СПРАВКА

по вопросу определения перечня перспективных информационных технологий для их инвестиционной поддержки и оценки информационной безопасности

(федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»)

Цифровая трансформация экономики характеризуется инновационными процессами внедрения информационных технологий во все сферы социально-политической и экономической жизни общества. Государство и корпорации инвестируют в информационные технологии значительные средства, что, в определенной степени, обуславливает экспоненциальный рост новых технических решений в этой области.

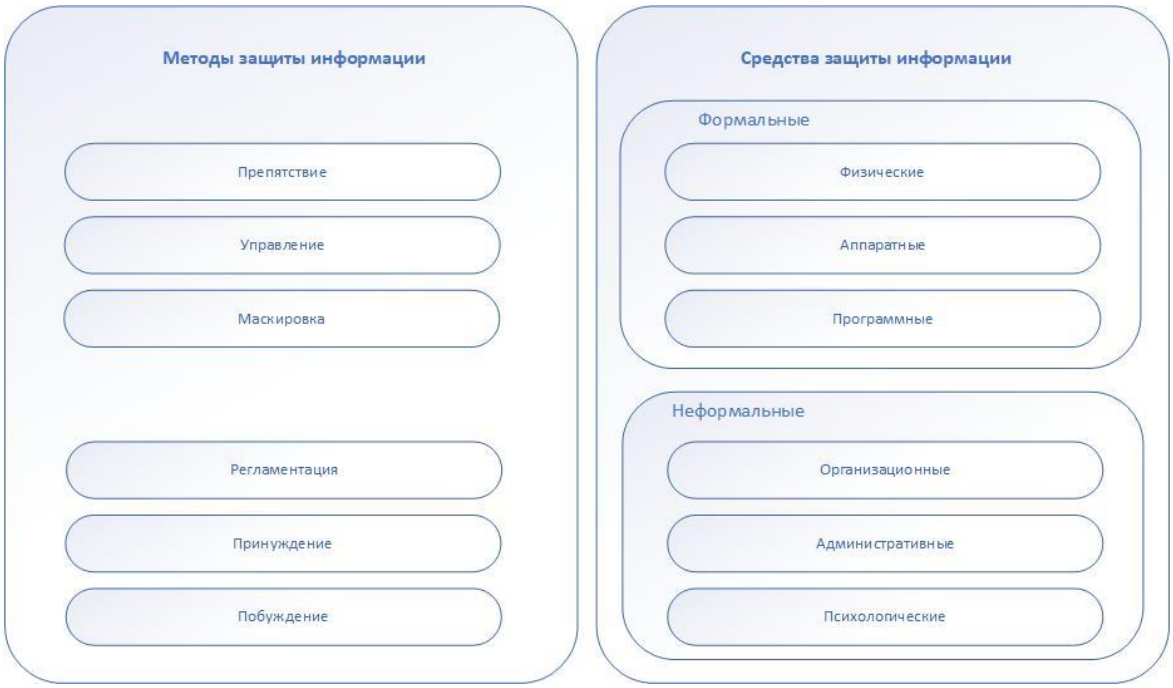
Инновационные решения требуют тщательного изучения в трех основных направлениях.

Во-первых, необходимо глубокое изучение новых технических решений с целью выявление в них различного рода уязвимостей. Из-за повышенного спроса и острой конкуренции многие инновации внедряются без должного тестирования на предмет информационной безопасности.

Во-вторых, новые технологии могут стать инструментом в руках злоумышленников для достижения ими своих противоправных целей, создавая новые, ранее не изученные вектора атак, дополнительный функционал по автоматизации процессов и увеличению масштабов и географии атак и новые механизмы обхода, существовавших ранее, средств защиты.

Во-третьих, инновационные технологии могут послужить основой для создания принципиально новой интеллектуальной системы информационной безопасности, в том числе как ответ на новые вызовы со стороны киберпреступности.

Большинство экспертов называют проблему кибербезопасности главным трендом современного развития IT-отрасли. Существующие решения в этой области реализуют различные методы обеспечения информационной безопасности, в связи с чем, рассматривая сквозные технологии как средства защиты информации, необходимо придерживаться их общепринятой классификации, которая как правило, выделяет формальные (технические) и неформальные (нормативные) средства. К неформальным средствам относятся административные (законодательные), нормативные (организационные) и морально-этические (психологические) нормы (стандарты, регламенты, корпоративная культура и прочее). К формальным относится физические, аппаратные и программные (специальные программные комплексы, оборудование, устройства и различные технические средства физической защиты).



Основные качества и примеры реализаций сквозных технологий для реализации различных методов обеспечения информационной безопасности приведены ниже.

Искусственный интеллект (ИИ)

Технологии искусственного интеллекта (ИИ) наиболее широко внедряются в различные системы информационной безопасности.

Кибератак не просто становится больше — они становятся сложнее. Злоумышленники проводят комплексные и многоступенчатые атаки. Например, некоторые нападения проводятся для того, чтобы отвлечь внимание специалистов по безопасности от другого участка информационной безопасности. У компаний возникает два пути: либо увеличивать штат отделов кибербезопасности, либо внедрять автоматизированные решения, которые учитывают сложность этих атак.

Человеческий фактор играет не маловажную роль в необходимости автоматизации процессов ИБ. Он может выступать как угроза, так и как уязвимость, характерные для всех видов кадров: от разработчиков, допускающих уязвимости в исходных кодах, до инженеров по безопасности, которые не всегда могут принять правильное решение во время атаки на ИТ-инфраструктуру, когда счет идет на секунды. Тогда как большинство инструментов ИБ все еще не реагируют на кибератаки, а лишь оповещают о них сотрудника департамента кибербезопасности и все важные решения всегда остаются за человеком задача автоматизации выходит на первый план.

Немаловажным фактором, влияющим на необходимость автоматизации процессов ИБ, являются технологии, которые становятся доступнее не только бизнесу, но и хакерам. Специалисты по кибербезопасности всегда «играют по правилам»: используют тот набор инструментов и регламентов, который принят в организации. У злоумышленника же регламентов нет: он использует все то, до чего сможет «дотянуться». В том числе, до технологий искусственного интеллекта. Если раньше злоумышленником атаковалась случайная выборка из базы, состоящей из тысяч организаций, то теперь с помощью искусственного интеллекта доступен сбор информации одновременно обо всех потенциальных целях и проводить адресные атаки на наиболее привлекательные или менее защищенные объекты.

Кадровый голод на рынке специалистов по ИБ отмечается в одинаковой степень как в России так за рубежом. Чем больше угроз, тем сложнее найти квалифицированного эксперта (особенно в регионах), и тем выше их зарплатные ожидания.

В сравнении с классическим подходом к средствам обеспечения ИБ, когда задействуются знания специалиста, технологии искусственного интеллекта и машинного обучения позволяют:

- обнаруживать ранее неизвестные атаки
- настраивать защитные инструменты без глубоких знаний
- принимать решения без перебора правил
- обрабатывать большие объемы данных и находить неочевидные закономерности, не доступные для анализа обычными методами.

К недостаткам можно отнести:

- необходимость большого объема данных и времени для обучения;
- сложность интерпретации полученных результатов;
- наличие ошибок первого и второго рода;
- ограниченность применения срезом обучающих данных.

Технология искусственного интеллекта может решать следующие задачи для целей обеспечения информационной безопасности:

- выявление аномалий (поведенческий анализ) – определение аномального поведения пользователей и сущностей, такие как использование нового устройства, обнаружение нового места положения или не характерное время использования;
- решение задач классификации - классификация данных, пользователей, источников угроз и вредоносного ПО;
- прогнозирование – прогнозирование и предсказание наиболее вероятных угроз, уязвимостей, рисков и векторов атак.

Основу технологии составляют алгоритмы, которые могут быть реализованы на различных языках программирования. При разработке

средств обеспечения информационной безопасности применяются различные алгоритмы. К примеру, в проекте с исходным кодом Spamassassin, который осуществляет фильтрацию спама на основе списка свойств почтовых сообщений, применяется Наивный Байес. В других системах применяются более продвинутые алгоритмы. Можно встретить такие алгоритмы как дерево решений, случайный лес, метод опорных векторов и др. Безусловно самым популярным в настоящее время является алгоритмы глубокого обучения. Это алгоритмы использующие многослойные нейронные сети.

Можно выделить следующие направления применения ИИ в ИБ:

- защита то атак отказа в обслуживании (DDoS);
- мониторинг трафика на уровне 7 модели OSI – уровне приложений (WAF);
- мониторинг сетевого трафика с выявлением и противодействием атакам (IDS/IPS, DLP);
- анализ поведения пользователей и сущностей (UEBA);
- сбор и корреляция данных о событиях ИБ (SOAR);
- детектирование и фильтрация спама;
- анализ фишинговых атак и мошенничества (fraud-detection);
- противодействие распределенным сетям вредоносных программных агентов (botnet);
- защита конечных устройств (EDR, sendbox) - выявление вредоносного кода в составе антивирусного программного обеспечения;
- обеспечение надежной идентификации и аутентификации;
- автоматизация реакций на инциденты и восстановление после аварий;
- предиктивная аналитика;
- компенсация нехватки кадров путем автоматизации различных процессов ИБ и обучения.

Некоторые специалисты особо выделяют направление Industrial Security Incident Manager (ISIM) - системы управления инцидентами, которые выявляют атаки и помогают в расследовании инцидентов на критически важных объектах.

Рассмотрим некоторые примеры таких применений технологии искусственного интеллекта более подробно.

Применение ИИ для защиты от DDoS атака возможно в трех направлениях.

Во-первых, это предсказание ожиданий пользователей. Динамическая подстрока пропускной способности на основе предсказания ожиданий и запросов пользователей. Идентификация природы всплесков повышенной загруженности каналов. Использование алгоритмов ИИ, которые могут интерпретировать большие объемы трафика, позволяет создать самоуправляемые сети, которые решают проблемы нагрузки до того, как это отразится на пользователях. Получая сведения из различных источников, в том числе социальных сетей, алгоритмы могут принимать решение об увеличении пропускной способности канала для надежной доставки контента пользователю или о блокировке вредоносной деятельности.

Во-вторых самодиагностика. Интеллектуальные алгоритмы на основе множественных показателей позволяют проводить самодиагностику и раннее обнаружение неисправностей для обеспечения наибольшей непрерывной работы. А в случае сбоев, позволяют в кратчайшие сроки провести устранение неисправностей.

В-третьих, поиск причин появления неисправностей. Алгоритмы ИИ способны в кратчайшие сроки обрабатывать большие объемы данных для помощи ИТ специалистам в определении сетевых компонентов, наиболее подверженных сбоям, что сокращает время устранения неисправностей.

Аббревиатура WAF образована от Web Application Firewall - защитный экран уровня приложений (L7), предназначенный для выявления и блокирования современных атак на веб-приложения, в том числе и с

использованием уязвимостей нулевого дня. Первые коммерческие WAF появились в 1999 году. Самый известный WAF с открытым исходным кодом - mod_security появился в 2002 году. Топологически, WAF обычно работают в режиме обратного прокси. Первые WAF использовали регулярные выражения, тогда как сейчас все больше внедряются алгоритмы искусственного интеллекта для обнаружения атак.

Мониторинг сетевого трафика с помощью средств искусственного интеллекта можно применять в сетях любого масштаба, от небольших офисов до сетей устройств, работающих в корпоративной среде. Автоматизированные средства способны заметить сканирование портов, множественные переходы хоста к хосту, нехарактерный траффик, передачу больших объемов данных и др. аномалии. Параллельно осуществляется собор всей соответствующей информации, ее анализ и дообучение модели многослойной нейронной сети. Благодаря этому достигается возможность надежно прогнозировать вероятность того, что тот или иной вид трафика окажется вредоносным в реальном времени. В качестве примера этого класса можно назвать продукцию Vectra Networks.

Для мониторинга поведения пользователей и систем (UEBA), а также для управления доступом используются различные продукты, хорошо зарекомендовали себя за рубежом продукт фирмы Aruba Networks (Hewlett Packard Enterprise). Важным свойством платформы Aruba является то, что она работает по принципу обучения без учителя. Атаки меняются и становятся все сложнее, например, в течение какого-то времени может иметь место малозаметная вредоносная активность, которая лишь позднее даст злоумышленнику возможность украсть большой объем данных, инструменты же машинного обучения помогают обнаружить подобное.

Модуль DLP-системы InfoWatch Prediction (класса UEBA), используя технологии машинного обучения, может анализировать аккумулированные в ИБ-системах большие данные и на их основе прогнозировать информационные риски для компании в сфере кадровой или финансовой

политики, в частности позволяет заранее определить намерение сотрудника уволиться. Таким образом решение способно частично выполнять функции как HR, так и ИБ-специалиста.

Технологии ИИ заложены в Enterprise Inspector решениях класса EDR, Sandbox и DLP от компании ESET, встроенная песочница ESET Dynamic Threat Defense, Офисный контроль и DLP Safetica.

Сбор и корреляция данных о событиях ИБ является актуальной темой как с точки зрения обеспечения комплексной защиты информации, так и с точки зрения соблюдения требований многих нормативных актов и требований регуляторов. Такой анализ необходимо выполнять быстро, сократив до минимума время между распознаванием и реакцией. Искусственный интеллект позволяет ускорить разбор инцидентов и тем самым улучшить понимание происходящего в корпоративной сети, точнее прогнозировать серьезные утечки, быстрее обнаруживать инциденты и оперативно реагировать на них, чтобы минимизировать возможный ущерб. В качестве примера можно привести продукцию Alert Logic.

Большие объемы информации об угрозах также собирают в GreatHorn, компании, являющейся оператором облачного сервиса безопасности электронной почты для Microsoft Office 365, Google G Suite и Slack. В организации накопилось более 10 Тбайт уже проанализированных данных по различным угрозам. Она используется для обучения модели на основе тензорного поля, что позволит обнаруживать взаимосвязи между различными видами сообщений, типами почтовых сервисов, сообщениями с разной тональностью высказываний и т. п.

Сервисы GreatHorn способны обнаруживать новые кампании фишинговых рассылок и переносить сообщения в карантин либо дополнять их предупреждениями за несколько дней до того, как исследователи придут к выводу о появлении новой угрозы. После идентификации такие сообщения могут быть автоматически удалены из всех почтовых ящиков, куда они были доставлены или перемещены на карантин.

Искусственный интеллект приходит на помощь и в случае детектирования вредоносного ПО в антивирусных системах. Классические системы просто не поспевают за создающимися каждый месяц вредоносными программами. ИИ обучается для обнаружения вирусов и вредоносного кода на основе технологий распознавания образов, что позволяет выявлять и изолировать подозрительную активность на самых ранних стадиях. ИИ может использоваться как самостоятельно, так и как инструмент прогнозирования для ускорения работы стандартных подходов.

Биометрические способы идентификации и аутентификации становятся все более популярными. С середины 2018 года биометрия начала в обязательном порядке применяться в банках. Помимо этого, она все чаще заменяет или как минимум дополняет ввод классических паролей доступа к системам и сервисам, используется в СКУД.

Технологии распознавания лиц нашли широкое применение в сфере безопасности. Так, в частности, британский банк Lloyds Bank тестирует технологию биометрической аутентификации, позволяющую клиентам входить в свой мобильный банк при помощи процедуры сканирования лица. А MasterCard с 2016 года экспериментирует с функцией, которую он называет “селфи-оплата". В том же году Amazon зарегистрировала патент на аналогичную платежную систему.

В Китае разрабатывается национальная система распознавания лиц, которая обещает идентификацию любого из 1.3 миллиарда жителей страны за 3 секунды. Проект, запущенный Министерством общественной безопасности КНР призван обеспечить потребности по обеспечению безопасности и правоприменительной практике. Система будет способна выявлять подозреваемых даже при массовом скоплении людей.

Системы ИИ могут использоваться как мульти-факторные системы аутентификации и контроля доступа. Реализуя политики контроля доступа интеллектуальные системы на основе анализа многих факторов могут в

режиме реального времени осуществлять динамический контроль прав доступа пользователей к защищенным активам.

Результаты исследований свидетельствуют, что в среднем на обнаружение атаки и реагирование на нее в организациях уходит 39 дней. Скорость реагирования напрямую зависит от уровня автоматизации, которая успешно обеспечивается средствами ИИ и машинного обучения, позволяя сократить это время до считанных часов.

Благодаря машинному обучению системы не только быстрее обрабатывают данные, но и коррелируют события, происходившие в разные периоды времени в разных регионах. Некоторые атаки могут повторяться через несколько недель или месяцев, при этом исходить из других сегментов. Искусственный интеллект может встать на защиту корпоративных интересов даже в случаях распределенной высококвалифицированной атаки.

Еще одна область применения искусственного интеллекта — предиктивная аналитика. Уже появились системы на базе искусственного интеллекта, которые прогнозируют наиболее вероятные виды атак на основе данных о предыдущих действиях киберпреступников, направленных на компанию.

Сегодня для определения критичности уязвимостей используют различные схемы подсчетов (например, CVSS) и калькуляторы. Все они не учитывают человеческий фактор, который может оказывать серьезное влияние. То, какие данные будут введены в калькулятор подсчета CVSS score, зависит от человека, который, как показывает практика, может быть подвержен влиянию извне. Например, если какую-то уязвимость активно обсуждают в медиа, то такая угроза может ему казаться более серьезной, или наоборот — недостаток информированности приведет к недооценке. Кроме того, вряд ли человек будет проводить повторный анализ спустя время. В результате возникают ситуации, как это было в случае уязвимости HeartBleed, чья базовая оценка CVSS изначально составляла всего лишь 5 из 10. При этом практически мгновенно стали появляться эксплойты для ее

использования — а значит, с самого начала риск был куда выше. Если доверить подсчет баллов CVSS обученной модели, то таких проблем можно избежать и получить постоянно обновляющуюся в зависимости от новых данных оценку критичности в данный момент.

Современные системы используют данные кибербразведки, одну или несколько платформ TI. Без них уже невозможно представить современный SOC. Технологии завтрашнего дня — это использование ИИ в выявлении взаимосвязей злоумышленников, построении графов, раскрывающих их скрытую инфраструктуру. Такие технологии позволяют вывести противодействие на качественно новый уровень. Например, в продукте Secure Bank - системе раннего обнаружения фрода для платежных систем, которая защищает 70 млн клиентов "Сбербанк Онлайн" и "Сбербанк Бизнес Онлайн", реализован разработанный специалистами Group-IB по DataSience алгоритм Behavior, позволяющий обнаружить мошеннические сессии на основании собранной информации о ранее осуществленных легитимных и мошеннических действиях. Система в автоматическом режиме определяет характерную последовательность действий для мошенников и для легитимных пользователей. Behavior проводит биометрический анализ клавиатурного почерка пользователя или почерка движения мыши и т.д. Система выявляет вредоносные веб-инъекции, социальную инженерию, фишинг, бот-сети, захват учетной записи, сети нелегального обналичивания денег и другие виды банковского мошенничества.

Чем более сложными становятся угрозы информационной безопасности, тем выше поднимается планка требований для тех, кто призван защищать свое предприятие. Более продвинутые инструменты защиты зачастую только усугубляют проблему кадрового голода, выявляя нехватку в штате сотрудников, обладающих необходимыми для эффективного использования новейших систем безопасности навыками. Этот вызов требует кардинально пересмотреть подход к созданию средств защиты и обеспечить механизмы ИИ, позволяющие радикально упростить работу подразделения.

Вопрос нехватки кадров стоит достаточно остро, поскольку для обеспечения безопасности постоянно изменяющихся бизнес-процессов в организациях необходимо непрерывно адаптировать правила, по которым работают сложные ИБ-системы (DLP, SIEM). Эта задача требует большого количества кадровых ресурсов, что приводит к увеличению стоимости владения системами безопасности. Именно поэтому внедрение искусственного интеллекта повышает эффективность ИБ-систем, снижает стоимость эксплуатации ИБ-решений, частично решает проблему нехватки кадров и позволяет автоматически решать прикладные задачи организации в этой сфере, к примеру в решении типовых задачах обслуживания информационных систем, первоначальной обработке запросов пользователей в техническую поддержку перед передачей их специалистам.

В качестве примера использования ИИ для обучения и повышения квалификации персонала можно привести генеративно-состязательные сети. В этом направление исследований используются одновременно две модели машинного обучения с противоположными целями. Одна решает задачу обнаружения, а другая – скрыть то же самое от обнаружения. Этим принципом пользуются при создании команд условного противника, чтобы выяснять, какими могут быть новые угрозы.

Системы искусственного интеллекта, применяемые в системах обработки естественного языка могут использоваться для сбора тематических сведений из открытых источников об актуальных кибер-угрозах, аномалиях и новых средствах обеспечения ИБ, повышая осведомленность соответствующих подразделений и руководства.

В последние годы значительно возросло количество стартапов и новых продуктов крупных игроков в области ИБ с применением ИИ. Можно привести большое количество примеров, которые внедрили технологии искусственного интеллекта в продукты для обеспечения информационной безопасности. К ним относятся такие, уже зарекомендовавшие себя игроки

рынка как Tanium, Cylance и LogRhythm и в прошлом успешные стартапы Darktrace, Harvest.AI, PatternEx, StatusToday и др.

Корпорации-гиганты тоже не остаются в стороне и применяют искусственный интеллект в сфере безопасности. Например, инженеры Google работает над системой на основе искусственного разума, которая будет создавать свое собственное шифрование, заменив тем самым полностью традиционную капчу. IBM запустили технологию Watson, Amazon приобрела Harvest.AI – обе системы используют алгоритмы для определения важных документов и IP, а затем анализируют поведение пользователей для распознавания возможных хакерских атак.

Компания Exabeam, лидер среди решений по поведенческому анализу пользователей UEBA, выпустила новое приложение для производителя программного обеспечения CrowdStrike, позволяющее специалистам по безопасности более эффективно выявлять различные аномалии и угрозы ИБ.

Банк Kotak Mahindra планирует инвестировать в развитие технологий на основе ИИ для выявления поведенческих аномалий пользователей. По словам руководителя службы безопасности банка, в условиях пандемии ключевыми требованиями стали безопасная работа из дома сотрудников и защита клиентов, которые вынуждены обслуживаться удалённо. Возросла нагрузка на цифровые сервисы банка. Между тем, мошенники стараются воспользоваться сложившейся ситуацией, что и определяет актуальность подобных разработок.

Компания Securonix представила новое решение SNYPR Security Analytics с функцией ResponseBot, которая предназначена для снятия нагрузки с аналитиков в области кибербезопасности. Securonix ResponseBot — основанный на искусственном интеллекте механизм, который помогает аналитикам справляться со сложными угрозами безопасности без необходимости привлечения специалистов высокой квалификации.

Компания Sensory заявила, что ее решение TrulySecure, специализирующееся на распознавании лиц и голосов, было

усовершенствовано для работы с пользователями, носящими медицинские маски. Предполагается, что новая функция будет востребована в свете условий, связанных с пандемией COVID 19. Кроме того, решение будет распознавать человеческий голос в шумных местах.

Компания «Лаборатория Касперского» активно встраивает модели машинного обучения в свои антивирусные продукты. Например, в программное решение Kaspersky Internet Security для Android был добавлен новый функциональный модуль, использующий для защиты мобильных устройств от цифровых угроз технологии машинного обучения и системы ИИ на базе нейронных сетей.

Компания Infosys использует технологии искусственного интеллекта для противостояния киберугрозам. Использование ИИ позволяет увеличить скорость реагирования на атаку и вывести работу в данном направлении на новый уровень. Обычно хакеры используют уже известные схемы нападения или создают новые на их основе. Искусственный интеллект наряду с машинным обучением использует информацию, связанную с прошлыми атаками, и быстро выявляет потенциальные риски, которые могут возникнуть.

Образовательные учреждения Великобритании все чаще используют технологии ИИ для защиты данных учащихся и результатов своих исследований. Об этом заявили представители Darktrace - одной из крупнейших ИИ-компаний в области кибербезопасности. Решения Darktrace выявляют аномальные действия, например, связанные с атакой, и прерывают их, не нарушая стабильную работу университетских систем.

Бюро переписи населения США планирует использование инновационных решений в области кибербезопасности в следующем десятилетии. Об этом говорится в плане крупнейшего национального статистического агентства, обнародованном 20 мая. Например, Бюро намерено уделить внимание рассмотрению возможностей искусственного

интеллекта и машинного обучения, чтобы перейти к анализу рисков кибербезопасности в реальном времени и отказаться от точечных оценок.

Национальный Банк Австралии использует биометрическое решение Nuance Gatekeeper для аутентификации клиентов. Разработка компании Nuance Communications позволяет быстро обнаруживать попытки мошенничества, улучшая клиентский опыт и укрепляя стандарты безопасности банка. Теперь миллионы клиентов мобильного банка могут быстро и безопасно попасть в систему без необходимости вводить пароль или отвечать на секретные вопросы.

Эффективная информационная безопасность требует высокоинтеллектуальных решений. Многие организации повышают степень своей защищенности за счет продуктов с использованием искусственного интеллекта. Эта тенденция внедрения ИИ позволяет продуктивно контролировать вредоносную активность и оказывать необходимую помощь ИБ подразделениям.

Виртуальная и дополненная реальность

Иммерсивная безопасность – это радикальный подход к использованию дополнительных средств визуализации как виртуальная реальность и голограммы для многомерной ситуационной осведомленности о состоянии сети. По мере роста угроз ИБ компаниям придется обратить внимание на интуитивно понятный характер иммерсивной безопасности, чтобы повысить комплексность подхода и сократить время реагирования на возможные инциденты, а также устранить растущий дефицит кадров, преследующий отрасль.

Технологии виртуальной и дополненной реальности могут применяться для обеспечения информационной безопасности в двух направлениях:

- как инструмент представления большого количества метрик и панелей индикаторов (дашбордов) для их анализа и принятия решений;
- как инструмент для обучения и тренировок.

В числе первых, иммерсивная безопасность была рассмотрена на конференции RSA в 2017 году. Докладчиками выступали представители компаний ProtectWise, Netflix, Lending Club и MN8STUDIO INC.

В последствии, расположенный в Колорадо поставщик облачного решения по обеспечению сетевой безопасности ProtectWise была приобретена телекоммуникационным гигантом Verizon Communications, цена сделки не разглашалась. Целью покупки было расширение предлагаемой линейки продуктов по обнаружению и реагированию на инциденты информационной безопасности. По заявлению экспертов это поможет Американскому поставщику телекоммуникационных услуг более прочно закрепиться на рынке услуг сетей пятого поколения 5G за счет возможности отслеживать сетевые угрозы и реагировать на них наиболее безопасным образом.

В одном из интервью, основатель ProtectWise рассказал, что они посветили 5 лет своей работы созданию инструментов обнаружения и реагирования нового поколения, которые помогут Verizon расширить свое портфолио услуг корпоративной безопасности.

Обеспечивая автоматизированное обнаружение и реагирование на угрозы любой сети, ProtectWise, реализовал ряд крупных проектов с такими компаниями как Jive, Motorola, Maxim Integrated, Pandora, Hulu, Netlogic, MGM Studios, Netflix, Nevada State College, Jumptrading, Universal Music Studio и другими.

При построении системы информационной безопасности организации все чаще используют в своей деятельности центры реагирования на критические инциденты (SIEM, SOC, SOAR). Внедрение технологий

виртуальной и дополненной реальности в эту среду позволяет существенно повысить эффективность этой работы.

В условиях быстро развивающихся технологий и растущего количества кибер угроз, очень важно найти более эффективные способы обнаружения и идентификации угроз и уязвимостей. Снижение сложности также позволит сотрудникам службы безопасности организации работать максимально эффективно. SOC помогают организациям, директорам по информационной безопасности (CISO) и их сотрудникам успешно анализировать, защищать и выполнять свои служебные обязанности по обеспечению кибербезопасности. Однако в их нынешней модели эти средства безопасности дороги, их сложно установить и поддерживать.

Технологии VR и AR могут помочь решить некоторые из проблем, с которыми сегодня сталкиваются SOC, позволяя организациям быстро мобилизовать и масштабировать свои центры без чрезмерных денежных и ресурсных вложений.

Использование виртуальной реальности в качестве платформы для сотрудников службы безопасности позволяет оперативно развернуть SOC в любом месте, освобождая их от ограничений физической инфраструктуры и географического положения традиционного центра. Выполнение действий из виртуального мира путем отправки серверных запросов из пользовательского интерфейса виртуальной реальности для управления средствами обеспечения информационной безопасности, запуска аналитики и разработки мер реагирования создает для пользователей единое пространство, в котором мониторинг и контроль существуют в одном виртуальном пространстве.

В среде виртуальной реальности роль аналитика безопасности первого уровня SOC может быть выполнена с помощью визуальных подсказок с соответствующим масштабом, не требуя глубоких знаний опытного специалиста по безопасности. Это позволяет организациям адекватно укомплектовать свои SOC перед лицом значительной конкуренции при приеме на работу и острой нехватки кадров на должности в области

кибербезопасности. Добавление услуг, таких как Watson for Cyber Security, еще больше расширяет эту возможность.

Несомненно, VR представляет собой смену парадигмы в том, как решения для мониторинга проектируются, создаются и используются. Виртуальная реальность несомненно является преимуществом для SOC организации: она может помочь снизить затраты, связанные с поддержкой SOC, обеспечить мониторинг более разнообразных источников и облегчить анализ большего числа конечных точек. Кроме того, виртуальная среда может повысить внутреннюю осведомленность о повседневных потребностях операторов SOC, помогая им определять области сосредоточения усилий по текущему обслуживанию экосистемы защиты.

Благодаря визуальному воздействию, виртуальная реальность предлагает уникальную среду, с помощью которой заинтересованные стороны бизнес-уровня могут быть в курсе экосистемы и состояния безопасности своей организации, повышая уровень доступности информации.

Интегрируя виртуальную и дополненную реальности с другими технологиями, такими как искусственный интеллект и роботизированные помощники (РПА), оператор SOC может выдавать голосовые команды для опроса определенных сетевых метрик без необходимости выхода из своей виртуальной среды. Это иммерсивное пространство виртуальной реальности позволяет специалистам по безопасности максимизировать время, потраченное на наблюдение за сетевой активностью и устранение потенциальных угроз, что, в свою очередь, обеспечивает более широкий угол обзора и позволяет генерировать более точные аналитические данные для высшего руководства.

Визуализация играет центральную роль в понимании данных экосистемы безопасности и ключевых показателей эффективности организации, а также для повышения внутренней осведомленности о состоянии безопасности организации сверху-вниз и удобном виде.

Организация не может отреагировать ни на инцидент, который не выражается в данных, ни на киберугрозу, которая скрыта в еще большем количестве данных или распределена во времени. В отчете Института Ponemon о вредоносных программах говорится, что самым большим препятствием для устранения атак повышенной сложности является недостаточная прозрачность событий, которые могут нести угрозу предприятию.

В отсутствии достаточной автоматизации аналитики безопасности тонут в данных, и им трудно на ежедневной основе интерпретировать поступающую информацию, особенно, когда большинство сообщений имеют высокий приоритет или уровень опасности. Увеличение количества панелей мониторинга и дисплеев не решает проблемы. VR может помочь эффективно организовать подаваемый материал и позволить сфокусироваться на выявлении потенциальных угроз и уязвимостей по мере их появления для наблюдения со стороны синей (защищающей) команды.

Ирландским отделением IBM был разработан прототип решения виртуальной реальности, интегрируемого с продуктом IBM QRadar SIEM с помощью платформы Unity Technologies - кроссплатформенного игрового движка, который можно использовать для создания интерактивных трехмерных пространств. Платформа Unity была объединена с прикладными программными интерфейсами (API) IBM QRadar SIEM для преобразования потока данных JavaScript Object Notation из приложения в форму трехмерной галактики внутри устройства с поддержкой виртуальной реальности.

Благодаря опыту геймификации для обучения вопросам безопасности и развития кибер-навыков, специалистами IBM было замечена огромная ценность использования визуальных метафор для объяснения сложных вопросов. На основе этого опыта они применили подход визуальной метафоры в своем прототипе виртуальной реальности для SOC.

Интегрированное в VR приложение IBM QRadar погружает специалиста по безопасности (синяя команда) в виртуальное трехмерное

пространство с планетами, звездами, туманностями, кометами и искусственными структурами. Каждый пространственный визуальный элемент представляет различные узлы ИТ-экосистемы оператора из решения SIEM, включая отдельные IP-адреса, базы данных, общедоступные конечные точки, ориентированные на клиентов, и другие информационные активы для отслеживания. Угрозы и предупреждения появляются в виде солнечных вспышек, сверхновых и других визуальных сигналов, четко предупреждая наблюдателя о любой потенциально опасной деятельности в области кибербезопасности в пределах отслеживаемой инфраструктуры.

В качестве другого примера использования VR в SOC можно привести решение, показанное на выставке RSA компанией Landrian Networks. Они активно используют VR для автоматизации работы SOCов с помощью очков Occulus путем визуализации различных процессов изучения угроз, расследования инцидентов, анализа поведения пользователей и т.п.

Дополненная реальность будет успешным развитием виртуальной, когда цифровой контент будет накладываться на реальное окружение SOC.

С помощью AR любой оператор на любом уровне может на лету накладывать друг на друга виды, чтобы дополнять представленные данные, улучшая прогнозирование, анализ и принятие решений. AR также является распространенной новой технологией со значительными преимуществами по сравнению с созданным прототипом VR. В случае SOC, AR может включать персонализированный и настраиваемый второй виртуальный экран (или представление) для каждого оператора.

В то время как главный недостаток SOC на основе VR заключается в том, что он уводит специалиста по безопасности из привычного физического мира в виртуальную среду, решение AR позволяет оператору SOC одновременно находиться в двух мирах.

Хорошо продуманный, настроенный и развернутый инструментарий интеграции VR и SIEM станет хорошим инструментом для организаций, создающих или поддерживающих будущие SOC. Несмотря на то, что

описанный выше прототип является виртуальным решением, продукты корпоративной безопасности со временем будут эффективно интегрироваться с дополнительной служебной программой дополненной реальности, чтобы способствовать более активному взаимодействию, самоотдачей и успеху внутри SOC.

Однако, по мнению некоторых специалистов, применение виртуальных, мобильных и территориально распределенных SOC в России может быть затруднено в связи с выходом 15.06.2016 Постановления Правительства РФ N 541, которое вносит изменения в Постановление от 3 марта 2012 г. N 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации», которое не позволяет аттестовать мобильное и динамично изменяющееся рабочее место по ГИС1.

В 2019 году на конференции RSAC компанией Inspired eLearning была представлена демо-версия программы повышения осведомленности персонала в вопросах ИБ, основанная на лучших практиках.

Демоверсия проводила посетителей выставки через различные сценарии по виртуальной безопасности и соответствию требованиям, основанные на лучшем в своем классе информационном материале по безопасности, подготовленном Inspired eLearning.

По мнению специалистов компании виртуальная реальность в обучении лучше имитирует реальные воспоминания обучаемого, как если бы виртуальный опыт был его собственным, и вызывает более сильные эмоциональные реакции, чем при традиционном обучении, и все это повышает усвоение информации. Такой метод является хорошим способом избавиться от стандартного курса электронного обучения, чтобы повысить интерес и мотивировать учащихся.

Они доказали, что обучение на основе виртуальной реальности способствует лучшему вовлечению в трудовой процесс и мотивации сотрудников. Inspired eLearning лидирует на рынке знаний о безопасности,

предлагая эту технологию в качестве нового способа обучения своих сотрудников для компаний.

Помимо демонстрации технологии VR, Inspired eLearning также продемонстрирует свой флагманский продукт Security First Solutions (SFS), доступный на 14 языках прямо из коробки, который недавно был удостоен двух серебряных наград на церемонии Cybersecurity Excellence Awards за образование в области безопасности в 2019 году Cybersecurity Excellence Awards for Security Education and Security Education Platform. В рамках платформы Security First Solutions компания Inspired eLearning также продемонстрировала свое решение PhishProof, единственный в отрасли инструмент для моделирования защиты от фишинга, способный обучить сотрудников распознавать весь спектр попыток фишинга на одной платформе: phishing (email), vishing (voice/phone), SMiShing (SMS text), USB baiting.

Информация с использованием виртуальной и дополненной реальности может подаваться в различных вариантах, представленных ниже.

Виртуальный аквариум. Виртуальный аквариум был представлен в 2017 году, когда с помощью Google Cardboard демонстрировалась контекстная база данных ИБ. Примером так же может служить продукт Personal Adventures, который создает впечатление виртуальной реальности, включая тактильную стимуляцию. Пользователь погружается в виртуальную реальность с помощью VR-очков и прослушивает короткую лекцию об опасности Интернета вещей. В виртуальной комнате, где, "крутя головой" вокруг, можно увидеть различные объекты (термостаты, часы, погодные станции, точки доступа, будильники, фитнес-браслеты и т.п.) и можно получить краткий обзор проблем с их безопасностью.

Интерактивный кинематограф. используют VR для автоматизации работы SOCов. Визуализируют различные процессы изучения угроз, расследования инцидентов, анализа поведения пользователей и т.п. В качестве примера можно привести продукт «Minority Report for the SOC».

Примером так же может служить продукт Holographic Challenge, который преподносит безопасность, ориентируясь на потребности бизнеса.

Виртуальный кинотеатр с помощью VR-очков показывает сложность современных атак и как они реализуются во временном промежутке (Spark Board).

Российская практика использования VR-технологий не менее обширна. Некоторые из ее применений ориентированы на общекорпоративную безопасность, но с легкостью могут быть адаптированы под нужды информационной безопасности. Так Сбербанк провёл тренировки инкассаторов с использованием VR-технологий. VR-тренажер, использованный в ходе тренировок, — разработка Лаборатории виртуальной и дополненной реальности и Службы инкассации Сбербанка.

Благодаря инновационной технологии VR-тренажер позволяет проводить ситуационные тренировки и имитировать стрельбу в условиях, максимально приближенных к реальным, а также проводить оценку действий сотрудников инкассации и охраны в многопользовательском режиме.

Технологии расширенной реальности могут помочь решить проблемы, с которыми сталкиваются современные SOC, позволяя организациям быстро мобилизовать и масштабировать свои центры без чрезмерных денежных и ресурсных вложений. Использование технологий виртуальной реальности в качестве платформы для сотрудников SOC позволяет им быть мобильными, отвлекая их от фиксированной физической инфраструктуры и географического расположения традиционного центра. В среде виртуальной реальности роль аналитика безопасности первого уровня SOC может быть выполнена с помощью визуальных подсказок соответствующей области действия, не требуя глубоких знаний опытного специалиста по безопасности.

Корпорация Vuzix, ведущий поставщик умных очков и устройств на основе технологии AR, совместно с разработчиком ПО NNTC объявила о том, что iFalcon Face Control Mobile, первая в мире полностью автономная система распознавания лиц на базе искусственного интеллекта,

интегрированная с интеллектуальными очками Vuzix Blade, была модернизирована до мощного и надежного решения, поддерживающего 4G и 5G. Смарт-очки iFalcon Face Control предназначены для сотрудников правоохранительных органов и охранников и позволяют сопоставлять лица в толпе с базой данных пропавших или подозреваемых людей. В очки встроена камера, которая позволяет владельцу сканировать лица прохожих и сравнивать с мобильной базой данных, содержащей 1 млн изображений. Обнаружив совпадение, устройство выводит уведомление на экран.

Центром исследований, разработок и разработок в области связи, электроники, США (CERDEC) разработаны очки Tactical Augmented Reality (TAR), которые внешне напоминают приборы ночного видения. TAR разрабатывалась по заказу для Министерства обороны США, но может использоваться в интересах подразделений обеспечения безопасности. Благодаря беспроводной связи между очками и специальным планшетом сотрудник органов безопасности получает информацию о своем местоположении, видит цель и расстояние до нее.

Компания Veative в партнёрстве с NASSCOM DSCI разработала концепцию использования виртуальной реальности в области кибербезопасности. Цель разработки концепции состояла в том, чтобы создать прототип визуализации сценария, в котором специалист по кибербезопасности мог бы легко идентифицировать возможные атаки и уязвимости в лабораторных условиях.

Целью генерального директора ProtectWise Скотта Часина и технического директора Джина Стивенса было создание полезного инструмента безопасности с интерактивной визуальной панелью, которая бы использовала визуальные эффекты заимствованные из кинематографа и компьютерных игр.

Компания, основанная в апреле 2013 года, выпустила Cloud Network DVR, виртуальную камеру в облаке, которая записывает все события сети

организации. Это позволяет специалистам по безопасности обнаруживать угрозы в режиме реального времени и проверять записанные исторические данные, чтобы обнаруживать угрозы, которые ранее были неизвестны, с использованием новейших аналитических данных.

Ядром решения является Wisdom Engine, который анализирует все данные сетевого трафика, анализируя сетевой поток с помощью глубокого анализа трафика (DPI), выявляя и классифицируя события ИБ, сопоставляя результаты со сведениями об угрозах из сторонних источников.

Особое внимание было уделено интерфейсу. Задачей было предоставить специалистам по безопасности полную и прозрачную картину их сети с возможностью быстро распознавать закономерности и взаимодействовать с огромными наборами данных.

Пользовательский интерфейс был назван ProtectWise Visualizer, а его создателем является Джейк Сарджант, профессионал по спецэффектам и визуальный дизайнер в MN8 Studio, ведущий художник анимационной графики для фильмов «ТРОН: Наследие» и «Обливион».

При работе по визуализации огромных наборов сетевых метрик авторы опирались на концепцию фильмов о полном погружении в среду данных, где визуализация осуществляется за счет сгенерированной компьютерной графики (CGI) и наложения. Это позволило предоставить пользователю ситуационную осведомленность в красивом интерфейсе, который предлагает как краткий обзор данных в масштабе, так и хороший инструмент, чтобы пользователь мог быстро, получив представление об общем состоянии сети, перейти в глубокое погружение по конкретному событию безопасности. Интерфейс предоставляет много сопутствующей информации и позволяет быстро распознавать образы, наблюдать за ними, распознавать закономерности и действовать без необходимости вчитываться. Таким образом была эффективно решена задача по обработке и предоставлению пользователю большого объема интуитивно понятных данных не перегружая его.

Визуальные эффекты индустрии развлечений ориентированы на создание зрелищности. В реальном продукте, таком как ProtectWise, это задача реализации гораздо более скрупулезного процесса понимания и последующей визуальной интерпретации данных для каждодневного использования с которой создатели успешно справились и продолжают совершенствовать свои разработки.

Фаза бета-тестирования решения началась в начале 2014 года и официально закончилась в апреле 2015 года. В нем приняли участие пятнадцать компаний разного размера и из разных отраслевых вертикалей, включая СМИ и развлечения, технологии, финансовые услуги и здравоохранение.

Одним из неожиданных и ключевых уроков, которые были извлечены в ходе тестирования, было то, насколько ценна всеобъемлющая видимость, которую пользовательский интерфейс ProtectWise обеспечивал не только аналитикам безопасности и лицам, отвечающим на инциденты, но и ценность, которую он обеспечивает для ИТ персонала. Для многих сотрудников, связанных с администрированием сети, это был первый опыт, когда они получили полную картину того, что происходит в их сети.

По мнению создателей ProtectWise большей части продуктов по обеспечению сетевой безопасности крайне не хватает наглядности и они не обеспечивают должный уровень прозрачности, необходимый профессионалам в области безопасности. Многие пользовательские интерфейсы больше напоминают интерфейсы для настройки маршрутизатора, чем для обнаружения сложных угроз и реагирования на них. Все большее количество сотрудников, особенно ИТ-специалистов, получают возможность пользоваться мощными визуализациями, которые можно найти в играх и они ожидают такого же подхода в услугах передовых технологий.

Применение VR/AR в кибербезопасности сделало большой скачок. Человеку свойственно анализировать причинно-следственные связи, и

виртуальная реальность легко позволяет реализовать такую возможность. В том числе и в кибербезопасности, где такие связи не всегда очевидны, а данных для их поиска слишком много. Правильная аналитика наряду с визуализацией позволит сильно облегчить эту работу.

Распределенный реестр (Блокчейн) (Blockchain)

Блокчейн получил широкую известность благодаря биткоину и криптовалютам. При этом возможности применения блокчейн в информационной безопасности поистине безграничны.

Блокчейн является одной из разновидностей распределенного реестра, обладающего следующими свойствами, которые успешно используются для обеспечения информационной безопасности:

- территориальное распределение;
- возможность вносить и хранить защищенные записи (транзакции);
- исполнение установленных политик, в отсутствии централизованного органа управления.

Национальный институт стандартов и технологий (NIST) выделяет следующие свойства:

- криптографически подписанные транзакции сгруппированы в блоки для формирования реестра;
- реестр защищен от несанкционированного доступа и обладает свойством неотказуемости т.к. каждый блок криптографически связан к предыдущей записью после соответствующей проверки.
- автоматически разрешает конфликты, используя установленные правила;
- репликация копий реестра в сети независимых узлов.

Рассмотрим некоторые свойства более подробно:

Блокчейн решает проблему отсутствия доверия между контрагентами на самом базовом уровне. В отличие от централизованной структуры, где вся информация хранится в нескольких очень больших базах данных, блокчейн - это распределенная база данных, используемая как в частных, так и в общедоступных приложениях. Данные, относящиеся к одному пакету действительных транзакций, хранятся в собственном блоке; каждый блок связан с предыдущим блоком, и постоянно увеличивается по мере добавления новых блоков информации.

Децентрализация - данные, содержащиеся в цепочке блоков, децентрализованы и проверены, поэтому при правильном распределении системы концепция единой точки отказа устраняется или другими словами, периметр для атаки сильно размывается, делая невозможным найти точку входа. Злоумышленник все еще может атаковать один из узлов структуры, но, чтобы нанести значительный ущерб, он должен атаковать более половины узлов блокчейна, что представляется весьма затруднительным. Благодаря этому инструменту любая создаваемая система по умолчанию достаточно устойчива.

Защита от взлома - каждый добавленный блок усиливает структуру блокчейна. Это связано с тем, что каждый блок содержит криптографическую ссылку на предыдущий блок, которая может быть изменена только с одобрения сетевых узлов: по мере роста структуры атакующему становится все труднее разорвать цепочку и получить контроль.

Шифрование и проверка – это две наиболее важные операции сетевой кибербезопасности. Блокчейн предлагает и то, и другое. Прежде всего, данные, представленные в цепочке блоков, зашифрованы и закодированы, а пользователь может расшифровать эти данные, используя свою систему ключей, которая является эксклюзивной только для него. Это дает дополнительный уровень безопасности и уверенность, что данные не были украдены, изменены или скомпрометированы. В блокчейн есть возможность проверить подписи файлов для всех записей с любых узлов, присутствующих

в сети. Таким образом, можно убедиться, что подписи подлинные и не были изменены.

Поддержание целостности данных в течение всего их жизненного цикла имеет решающее значение в информационных системах и является одной из задач информационной безопасности. Шифрование данных, сравнение хэшей (дайджест данных) или использование цифровой подписи - вот некоторые примеры средств, которые могут использоваться для обеспечения целостности данных, независимо от стадии, на которой они находятся (в пути, в состоянии покоя и в используемом хранилище). Рассматриваемые характеристики, такие как неизменяемость и прослеживаемость блокчейна уже предоставляют необходимые средства для обеспечения целостности данных.

Комбинация последовательного хеширования и криптографии вместе с децентрализованной структурой делает очень сложным вмешательство любой стороны в блокчейн, в отличие от стандартной базы данных. Это дает уверенность в целостности и достоверности данных. Протоколы модели консенсуса, связанные с технологией, дополнительно повышают уровень уверенности в безопасности данных, поскольку обычно 51% пользователей в публичных и частных блокчейнах должны согласиться с тем, что транзакция действительна, прежде чем она будет добавлена в цепочку. Так же существует возможность внедрить дополнительные механизмы для предотвращения и контроля разделения реестра на случай атаки «кибер-контроля 51%», например, отслеживать, увеличившуюся вычислительную мощность одного из узлов или выполнение значительно большего количества транзакций.

Прослеживаемость – неотъемлемое свойство блокчейна делающая его столь популярным и универсальным средством. Каждая транзакция, добавляемая в частную или публичную цепочку блоков, имеет временную метку и цифровую подпись. Это означает, что можно отследить конкретный

период времени для каждой транзакции и найти соответствующую сторону в цепочке блоков через свой публичный адрес.

Это свойство тесно связано со свойством неотказуемости: уверенность в том, что никто не сможет отказаться от подлинность своей подписи в файле или авторства транзакции, которую он инициировал. Такая функциональность цепочки блоков повышает надежность системы в целом, поскольку каждая транзакция криптографически связана с пользователем.

Любая новая транзакция, которая добавляется в цепочку блоков, приводит к расширению глобального состояния реестра. Это означает, что при каждой новой итерации системы предыдущее состояние будет сохраняться, в результате чего журнал истории полностью прослеживается.

Возможность аудита блокчейна является неоспоримым преимуществом, повышающим безопасность и прозрачность каждой итерации. С точки зрения кибербезопасности это дает дополнительный уровень уверенности в том, что данные не были подделаны и являются подлинными.

Доказательство с нулевым разглашением — это концепция защиты данных, требует наличия интерактивных исходных данных от проверяющего, как правило, в виде задачи или проблемы. Цель легального доказывающего (имеющего доказательство) в этом протоколе — убедить проверяющего в том, что у него есть решение, не выдав при этом даже части «секретного» доказательства («нулевое разглашение»). Цель проверяющего же — это удостовериться в том, что доказывающая сторона «не лжёт». К примеру, речь может идти о проверке личности человека без использования его личных данных - вместо этого это делается путем проверки того, что он соответствует определенным требованиям. Если эта концепция хорошо проработана, она значительно повышает степень защищенности.

Одноранговый обмен - это еще одно важное свойство транзакций Blockchain. Это означает, что данные совместно используются одним пользователем и принимаются одним пользователем, используя миллионы

узлов, присутствующих в сети, и ключи, назначенные обоим пользователям Blockchain. Это гарантирует отсутствие сбора или передачи данных по какому-либо одному единственному каналу. Одноранговый обмен позволяет Blockchain исключить посредника из процесса обмена и прохождения транзакций, в том числе поставщиков услуг. Один пользователь делится информацией с широко распространенной сетью Blockchain, а получатель получает ее, используя свой уникальный ключ, без вмешаьельства какого-либо третьего лица. Это не только ускоряет процесс, но и во много раз повышает безопасность совместно используемых ресурсов.

Для использования технологии в качестве средства обеспечения информационной безопасности можно рассматривать как публичные так и приватные блокчейн.

Публичные блокчейны позволяют любому человеку или системе:

- доступ и просмотр реестра;
- вносить предложение на добавление новых блоков данных в реестр;
- подтверждать транзакции, следуя установленным протоколам.

Публичные блокчейны имеют структуру административного управления, но обычно работают без какого-либо центрального органа. Примеры общедоступных блокчейнов включают большинство криптовалют, таких как Биткойн и Эфириум.

Частные блокчейны ограничивают доступ к реестру определенным известным или доверенным сторонам, которые обычно должны участвовать, используя свои подлинные проверенные личности. Они полагаются на структуру управления и полномочия, чтобы осуществлять:

- контроль доступа к реестру;
- реализацию функций и соответствующего кода для их поддержки, например, внедрение смарт-контрактов или транзакций в цепочке поставок;
- применение и контроль соблюдения правил;

- реагировать на инциденты, включая киберугрозы.

Вариант применения публичного блокчейна поддерживает самое большое количество участников, мало или совсем не знающих друг друга. Однако отсутствие конфиденциальности и невозможность ограничить количество участников публичной цепочки блоков могут создать неприемлемый уровень риска для некоторых бизнес-транзакций. Организации, которые хотят сотрудничать, не подвергая свои транзакции и бизнес-процессы публичному контролю или ограничить круг участников, могут успешно внедрять совместные разработки частных приложений блокчейна. Например, решение IBM Food Trust - это сеть на основе блокчейна, которая включает Walmart и других участников цепочки поставок продуктов питания для точного и безопасного отслеживания продукции от фермы к столу.

Благодаря своим свойствам технология может применяться в следующих областях для обеспечения информационной безопасности:

- для поддержки надежного обмена информацией о кибербезопасности между широко распределенными несвязанными организациями;
- для проверки достоверности и конфигурирования программного обеспечения;
- для использования списков доверенных компонентов;
- для получения информации из проверенных источников для обнаружения вредоносных программ или атак;
- для построения распределенных реестров идентификации;
- для заключения смарт-контрактов;
- как решение для цепочки поставок;
- публичные записи, такие как реестры собственности;
- и другие приложения, особенно те, которые требуют совместного использования удостоверенных данных между несколькими географически распределенными сторонами.

Далее будут рассмотрены обобщенные варианты применения и конкретные реализации блокчейн для целей обеспечения информационной безопасности.

Данная технология может быть применена как мера контроля такого риска как человеческий фактор.

Организации могут аутентифицировать устройства и пользователей без необходимости ввода пароля с помощью технологии блокчейн. Это исключает вмешательство человека в процесс аутентификации, тем самым исключая потенциальный вектор атаки.

Использование централизованной архитектуры и простых входов в систему - большая слабость обычных систем. К примеру, все усилия будут напрасными, если сотрудники или клиенты будут использовать слабые пароли, которые легко украсть или взломать. Блокчейн предлагает надежную аутентификацию и одновременно устраняет единую точку атаки.

С помощью блокчейна система безопасности, используемая в организации, может использовать распределенную инфраструктуру открытых ключей для аутентификации устройств и пользователей. Эта система безопасности предоставляет каждому устройству определенный сертификат SSL вместо пароля. Новшеством является то, что управление сертификатами может осуществляться через блокчейн, что делает практически невозможным использование злоумышленниками поддельных сертификатов.

Кража личных данных становится серьезной проблемой в наше время. Киберпреступники используют чужую личность для совершения преступлений, но с внедрением технологии блокчейн эту практику можно предотвратить. Применяя специализированное приложение, к примеру, можно организовать децентрализованную среду для обеспечения доступа к действиям и транзакциям с любого устройства. Таким образом, каждая завершенная транзакция будет регистрироваться при всеобщем одобрении.

В настоящее время в большинстве приложений для обмена сообщениями отсутствует стандартный набор протоколов безопасности, а также унифицированная структура API, позволяющая осуществлять обмен данными между мессенджерами. Развивающиеся безопасные коммуникационные экосистемы блокчейнов встают перед лицом этой проблемы и работают над созданием единого интерфейса. Технология блокчейн - отличное решение для этого, поскольку она защищает все обмены данными и обеспечивает связь между различными платформами обмена сообщениями, а более новые сети, такие как Bitcoin Cash, обещают передавать гораздо больше информации на каждый блок, приближая нас к системе децентрализованной связи.

Система доменных имен (DNS) является частично децентрализованной системой сопоставления «один-в-один» и ассоциирует имена доменов с их сетевыми адресами. На данный момент блокчейн является единственным возможным решением для предотвращения DDoS-атак, связанных с DNS и это одна из главных причин, по которой технологические гиганты выбрали блокчейн как средство обеспечения информационной безопасности.

Внедрение технологии блокчейн полностью децентрализует DNS, распределяя содержимое по большему количеству узлов, тем самым делая практически невозможными атаки на эту службу. Используя цепочки блоков, система будет неуязвима для злоумышленников, до тех пор, пока не будет выведено из строя достаточно большое количество узлов одновременно.

Права на редактирование домена в этом случае будут предоставляться только владельцам домена, и никакой другой пользователь не сможет вносить изменения, что в значительной степени снижает риск доступа к данным или их изменения посторонними лицами.

Некоторые компании уже внедряют блокчейн, чтобы защититься от DDoS-атак. Например, Blockstack предоставляет возможность создать полностью децентрализовать компьютерную сеть. Концепция компании заключается в том, чтобы сделать всю всемирную сеть децентрализованной,

исключив всех третьих лиц из управления веб-серверами, системами идентификации и базами данных.

Смарт-контракты, (интеллектуальные контракты) реализованные на базе локальных приложений, работающих в реестре, сегодня стали ключевой особенностью блокчейнов. Этот тип программы может использоваться для упрощения, проверки или обеспечения соблюдения правил между сторонами, предлагая четкое исполнение и взаимодействие с другими смарт-контрактами.

Крупнейший финансовый институт в США J.P.Morgan, разработал на основе Ethereum платформу под названием Quorum. Платформа использует технологию блокчейна для обработки транзакций. Банк использует интеллектуальные контракты в сети Quorum для осуществления прозрачных, но криптографически защищенных транзакций.

Процедуры обновления программного обеспечения и установки приложений из доверенных источников являются неотъемлемой частью любой системы по управлению информационной безопасностью. Технология блокчейн может выступать как средство обеспечения безопасности этих процедур.

Вредоносное ПО является одной из наиболее актуальных угроз, которые проявляются в разных формах. Их становится сложно идентифицировать даже с использованием средств защиты конечных узлов (EDR). Зачастую, программы-вымогатели и вредоносные программы маскируются под легальные приложения. Блокчейн может предоставить надежный механизм доставки хэшей для контроля целостности и аутентичности обновлений и загрузок, что полностью исключит возможность загрузки вредоносного кода.

Индустрия 4.0 и 5G - это области цифровой трансформации, которые создадут важные перспективы для кибербезопасности, прежде всего в области Интернета вещей. С широким внедрением 5G Интернет вещей станет повсеместным. Каждый день миллионы устройств будут требовать

аутентификации и подключения к централизованным системам. Блокчейн может быть полезен как для аутентификации, так и для выявления компрометации устройств. Источники приводят новую парадигму – Интернет безопасных вещей (IoTT), которые должны использовать следующие механизмы:

авторизация устройств – устройства должны идентифицировать друг друга, устанавливать доверенные соединения и выявлять устройства нарушители;

обеспечение надежности - архитектура Интернета вещей обычно использует центральный орган для управления устройствами и данными, которые они генерируют. Технология блокчейн позволяет отдельным узлам или устройствам быть более независимыми. Например, каждое устройство IoTT, участвующее в сети с поддержкой блокчейна, может: иметь достоверную политику поведения; выявлять, помечать и помещать в карантин устройства с необычным поведением для проверки системным администратором или другим органом.

Большинство систем IoT управляются с помощью микропрограмм, поэтому обеспечение целостности и аутентичности обновления микропрограмм устройств - сложная и важная задача, которую необходимо тщательно решать. Кроме того, может случиться так, что несколько устройств с их различными подсистемами потребуется срочно и одновременно обновить, например, чтобы применить критическое исправление. Следовательно, требуется высокая доступность обновлений.

Большинство существующих решений для обновления микропрограмм зависят от модели клиент-сервер, в которой производитель делегирует процесс распространения микропрограмм поставщикам своей продукции. Недостатком центральной клиент-серверной архитектуры является наличие единой точки отказа (SPoF), и в случае, если сервер недоступен, устройства IoT не могут получить доступ к ресурсам (обновлениям). Рассмотрим два возможных подхода: ручной и автоматический.

В процессе обновления вручную, владелец устройства должен запустить процесс обновления прошивки. Как правило, этот тип обновления применяется на устройствах с ограниченной пропускной способностью. Однако механизм обновления прошивки вручную не эффективен по многим причинам таким как многообразие устройств и недостаток квалификации владельцев. Кроме того, высока вероятность того, что в процессе обновления прошивки может произойти человеческая ошибка, электрический сбой или элементарное несоответствие устройства обновления в связи с устареванием.

Автоматическое обновление сегодня кажется более подходящим. Предпочтительно, что бы производитель устройства IoT сам проводил обновление прошивки без активного участия владельца устройства. Текущий процесс автоматического обновления прошивки использует архитектуру клиент-сервер, где репозиторий поставщика является сервером, а устройство IoT становится клиентской стороной. Как правило, существует два способа доставки микропрограммы с сервера на клиент: методы PUSH и PULL. Различия между этими двумя методами заключаются в инициаторе процесса обновления. В методе PUSH производитель устройства запускает процесс обновления прошивки, распространяя двоичный файл прошивки, в методе PULL устройство IoT запрашивает процесс обновления прошивки, отправляя двоичный запрос на загрузку прошивки на сервер.

Технология блокчейн могла бы использоваться для проверки версии прошивки и файла подлинности прошивки, а также для распространения двоичного кода прошивки на узлы, подключенные к сети. Каждое устройство IoT является сетевым узлом, а каждый узел должен хранить всю цепочку или ее часть в своем локальном хранилище, что не совсем подходит для устройств с ограниченными вычислительными ресурсами.

В другом варианте устройство IoT должно периодически проверять любой случайный узел в блокчейн-сети, чтобы проверить версию прошивки. Когда поставщик устройства публикует новую версию обновления прошивки в блочной сети, вновь созданное обновление прошивки должно быть сначала

проверено сетью по протоколу консенсуса. Затем, когда одно из IoT-устройств соответствующего поставщика устройства хочет выполнить процесс обновления прошивки, устройство должно создать транзакцию для запроса обновления прошивки. В этой схеме устройства IoT не смогут загрузить прошивку, если большая часть узлов в сети не одобрили ее.

Блокчейн может успешно применяться для реализации стратегий резервного копирования и восстановления. Система резервного копирования и восстановления должна соответствовать следующим характеристикам:

Непрерывное или автоматическое резервное копирование данных: гарантирует, что изменения, которые вы вносите в свои файлы, одновременно копируются в место хранения. Это позволяет восстанавливать даже самые последние изменения в случае потери данных, что приближает целевую точку восстановления.

Инкрементное резервное копирование: это тип резервного копирования, при котором копируются только изменения, а не весь файл. Это сокращает время, необходимое для копирования данных, и не замедляет основную работу.

Мгновенное восстановление: эта функция подразумевает запуск текущего снимка резервной копии на вторичном инстансе, чтобы сократить время простоя приложения при переключении от основного на резервное.

Дедупликация данных: исключает повторяющиеся блоки записи данных при переносе данных в хранилище резервных копий. Это снижает нагрузку на сеть и необходимое пространство для хранения.

Безошибочное копирование: функции программного обеспечения резервного копирования данных также гарантируют, что данные, скопированные из источника и сохраненные на сервере резервного копирования, являются одинаковыми и не содержат ошибок и несовпадений.

Все они успешно реализуются с помощью технологии блокчейн.

Еще один вариант использования блокчейна для обеспечения информационной безопасности это анализ угроз. Анализ угроз - это процесс,

который включает в себя сбор ценной информации, включая механизмы, контекст, индикаторы, практические советы и выводы о возникающей или существующей киберугрозе. Процессы анализа угроз необходимо адаптировать к экосистеме организации, чтобы правильно интегрировать ее.

Одна из проблем, связанных с интеллектуальным анализом угроз в наши дни, заключается в том, что компании обычно тратят много времени на изучение одних и тех же угроз, в то время как другие остаются незамеченными. Как следствие, появляются новые тенденции, которые имеют решающее значение для возможности обмена информацией между различными заинтересованными сторонами. Следуя этому принципу, разные компании как потребители услуг SOC так и поставщики могут обмениваться информацией об угрозах в интересах друг друга создавая и дополняя распределенный реестр применяя блокчейн, решая задачу синхронизации между различными сторонами.

В качестве примера, уделяя особое внимание надежным экосистемам, европейская инициатива пытается реализовать платформу управления угрозами на основе блокчейна, которой является проект SPHINX. В этом проекте, медицинские устройства Интернета вещей в разных медицинских центрах обмениваются информацией о различных угрозах, в идеале затрагивающих одну и ту же экосистему. Различные компоненты в рамках одного проекта читаются из одного реестра, поэтому все они имеют единое представление данных. Инфраструктура блокчейна действует как BaaS (блокчейн как услуга), узлы которого находятся в разных медицинских центрах, а различные устройства IoT выступают в качестве пользователей этой общей платформы.

Мониторинг и ведение журналов так же можно обезопасить с использованием рассматриваемой технологии. Проводятся исследования, в которых блокчейн применяется для улучшения систем регистрации. В качестве примера, можно привести решение для европейского проекта Sunfish на основе распределенной базы данных, которая обеспечивает

целостность данных и стабильность системы. Специалистами анализируются преимущества и недостатки использования этого инструмента путем реализации облачных вычислений. Nokia Bell Labs опубликовала небольшой отчет, в котором предлагается использовать частные блокчейны вместо общедоступных для управления журналами.

В здравоохранении технология распределенного реестра используется для защиты данных о пациентах больниц. Распределенный реестр позволяет только определенным допущенным лицам иметь доступ к ограниченным объемам информации, которые, если их объединить, составили бы всю медицинскую карту пациента.

Компания Hashed Health внедряет технологии блокчейна и сотрудничает с десятками медицинских компаний и больниц для создания безопасных цифровых цепочек блоков для обмена информацией о пациентах по внутренним каналам связи.

Появился первый опыт использования технологии блокчейн на правительственном уровне. Пионером в этой области является Австралия, где в партнёрстве с компанией IBM была создана блокчейн-экосистема для безопасного хранения правительственных документов.

Рассматривая вопросы обеспечения информационной безопасности, нельзя забывать о соблюдении законодательства и регулятивных требований. Для соответствия законам о конфиденциальности данных, блокчейн позволяет реализовать право на забвение. С одной стороны, технология гарантирует, что ничего не будет стерто, но личная информация, записанная в системе, зашифрована и нормативные требования могут быть соблюдены с использованием механизма устаревания или отзыва ключей, что приведет к тому, что конфиденциальная информация станет недоступной.

Несомненно, технологии блокчейн являются эффективным инструментом для реализации средств обеспечения информационной безопасности.

Инновационное использование блокчейнов уже становится неотъемлемым компонентом других областей, помимо криптовалют и повышение кибербезопасности не является исключением.

Подводя итог, можно сказать, что блокчейн полезен при обмене информацией между разными сторонами. Независимо от того, хотим ли мы идентифицировать эмитентов этой информации или хотим их анонимизировать.

Квантовые технологии (Quantum Technology)

В настоящее время квантовая информатика представляет собой новую, быстро развивающуюся отрасль науки, связанную с использованием квантовых технологий для реализации принципиально новых методов инфо-телекоммуникации и вычислений: квантовая информация, квантовая информатика, квантовые каналы связи, квантовая криптография, квантовый компьютер.

Квантовая информация – это физическая величина, характеризующая изменения, происходящие в системе при взаимодействии информационного потока с внешним окружением. Квантовая информация — это новый вид информации, который можно передавать, но нельзя размножить. Квантовый бит или ку-бит описывается единичным вектором в двумерном комплексном векторном пространстве и представляет собой двухуровневую квантовую систему. В качестве ку-битов могут выступать ионы, атомы, электроны, фотоны, спины атомных ядер, структуры из сверхпроводников и многие другие физические системы.

Развитие квантовых технологий послужили основой для создания принципиально новых систем защиты информации. Работы по совершенствованию технологий информационной безопасности ведутся в направлениях квантовой и постквантовой криптографии.

В свою очередь эти два направления можно разделить на под-домены. В вопросах постквантовой криптографии рассматриваются проблемы существующих алгоритмов шифрования с точки зрения квантовой угрозы и разработки квантово-стойких алгоритмов.

В области квантовой криптографии для обеспечения информационной безопасности можно выделить направления:

- квантовые коммуникационные технологии – квантовые криптографические системы выработки и распределения ключей;
- технологии квантовой обработки информации – системы квантового шифрования и квантовые генераторы случайных последовательностей;
- технологии квантовых вычислений – квантовые компьютеры и алгоритмы, квантовый криптоанализ.

Прежде чем переходить к рассмотрению этих направлений, рассмотрим особенности технологии, оказывающие на них влияние.

В основе квантовой информатики и квантовых вычислений лежит понятие квантового бита (ку-бит – частный случай ку-энка, который может иметь формы ку-трита, ку-дита и др. bipartite entanglement of qubits), который является в некотором роде аналогом классического бита. Особенностью ку-битов является то, что они имею два квантовых состояния и находятся в суперпозиции т.е. могут одновременно находится в обоих этих состояниях. Другими словами, состояние ку-бита невозможно определить обозревая его, он находится одновременно в двух состояниях, до тех пор, пока его состояние не измерено. Квантовые состояния характеризуются вероятностями, называемыми амплитудами, описываемыми комплексными числами. Квантовые вычисления — это трансформация квантовых вероятностей.

Математически суперпозиция представляет собой линейную функцию (комбинацию) вероятностей квантовых состояний ку-бита. При выполнении унитарных операций над n-кубитовой квантовой системой, которая

находится в состоянии суперпозиции, происходит одновременная обработка всех 2^n возможных состояний. Именно этот эффект, который получил название квантовый параллелизм, позволяет хранить большое количество информации и дает значительное ускорение вычислительного процесса.

Как видно, квантовые вычисления носят вероятностный характер, чем отличаются от классических детерминированных вычислений. К ним не применимы классические алгоритмы логических операций И, ИЛИ и др. Поэтому для каждого применения квантового компьютера должны быть разработаны свои математические алгоритмы.

Алгоритмы шифрования построены на математических проблемах сложно решаемых с использованием обычных компьютеров, но решаемых с помощью квантовых вычислений с экспоненциальным ускорением.

Например, алгоритм QAOA (Quantum Approximate Optimization Algorithm) может превзойти классический компьютер со 100-200 кубитами и очень малой глубиной схемы (грубо говоря малым количеством логических вентилей), поэтому квантовая коррекция ошибок строго не требуется. Это также причина, по которой QAOA является одним из кандидатов на демонстрацию квантового превосходства.

Алгоритм Шора обеспечивает экспоненциальное ускорение решения задач факторизации, дискретного логарифма (DLP) и дискретного логарифма с эллиптической кривой (ECDLP), которые широко используются в криптографических приложениях. Будь то TLS, SSH или IPSec, наиболее безопасные протоколы связи так или иначе полагаются на соглашения о ключах Диффи-Хеллмана (которые зависят от стойкости DLP или ECDLP), на цифровые подписи (DSA, ECDSA или RSA-PSS подписи) или на шифрование с открытым ключом (Эль-Гамаль, RSA-OAEP). Таким образом, алгоритм Шора потенциально нарушает все эти алгоритмы, а вместе с ними и все механизмы криптографии с открытым ключом, развернутые в Интернете.

С другой стороны, чтобы реализовать алгоритм Шора для разложения 2048-битного числа, потребуется более 4000 стабильных кубитов и

миллиарды логических вентилей. Поскольку продолжительность такого вычисления будет намного больше, чем время, в течение которого кубиты могут оставаться стабильными (время когерентности), требуются другие методы для поддержания информации в кубите. Эти методы, такие как квантовая коррекция ошибок, пока не реализуемы при нынешних возможностях квантовых компьютеров. Следовательно, даже самые оптимистичные прогнозы оценивают период в 10 лет до первой демонстрации алгоритма Шора на 2048-битном числе.

В настоящее время показано, что на квантовом компьютере принципиально можно решить любую математическую задачу. Вопрос в том, насколько эффективно по времени будет это решение. Известные эффективные квантовые алгоритмы можно условно разделить на две группы: дающие экспоненциальный выигрыш (например, алгоритм Шора) и дающие квадратичный выигрыш (например, алгоритм Гровера). В связи с тем что класс задач, решаемых квантовыми алгоритмами за полиномиальное время, пока не удается существенно расширить, большое внимание уделяется анализу алгоритма Шора и других полиномиальных алгоритмов с целью выявления общности и важнейших свойств этих алгоритмов, а также соответствующих задач, позволяющих добиться полиномиальности.

Сегодня можно утверждать также, что в эффективные квантовые алгоритмы может быть трансформирован ряд современных алгоритмов в области алгебраической геометрии и алгебраической теории чисел. Например, упоминавшееся выше разложение на простые множители целого числа квантовый компьютер может выполнять экспоненциально быстрее, чем классический. Интересны с точки зрения криптографических приложений исследования по оценке трудоемкости квантового алгоритма дискретного логарифмирования Шора для случая группы точек эллиптической кривой, определенной над конечным простым полем. В РФ впервые было показано, что применение нового метода для определения вероятности успеха в этом квантовом алгоритме позволяет сократить почти в

100 раз первоначальную оценку Шора для числа итераций алгоритма дискретного логарифмирования. Кроме того, впервые удалось получить оценки трудоемкости реализации квантовых алгоритмов дискретного логарифмирования применительно к стандартам электронной подписи ГОСТ Р34.10-94 и ГОСТ Р34.10-2001.

Много потенциальных приложений имеет алгоритм квантового поиска. Так, его можно использовать для более быстрого, чем на классическом компьютере, нахождения статистик (например, наименьшего элемента) в неупорядоченном наборе данных. С его помощью можно ускорить алгоритмы для решения некоторых задач класса NP – тех задач, для которых неизвестен лучший алгоритм, чем прямой перебор. Наконец, его применение позволяет ускорить поиск ключа к таким криптосистемам, как широко известный алгоритм DES. Квантовое преобразование Фурье также имеет много интересных приложений. С его помощью можно решить задачи вычисления дискретного логарифма и факторизации. Это, в свою очередь, и позволяет "взломать" с помощью квантового компьютера многие из наиболее популярных криптосистем, включая RSA.

Алгоритм Гровера - это поиск в несортированном списке. Это общий метод, который можно применить ко многим типам вычислительных задач. Обратной стороной этого алгоритма является то, что он предлагает более ограниченное ускорение, чем, например, Алгоритм Шора. Ожидается, что результаты этого алгоритма не будут такими впечатляющими, как другие алгоритмы, но, тем не менее, важны для некоторых приложений.

Интересен алгоритм квантового перечисления. Этот алгоритм, представляющий собой комбинацию из квантового поиска и преобразования Фурье, может быть использован для более быстрой, чем это возможно в случае использования классического компьютера, оценки числа решений задачи поиска.

QAOA (Quantum Approximate Optimization Algorithm) это общий метод решения задач оптимизации при определенных условиях. Многие проблемы

в области финансов, производства, транспорта и т.д. можно сформулировать как задачу оптимизации, что показывает потенциал этого алгоритма.

Алгоритм Харроу Хассидима Ллойда (HHL) это алгоритм, который решает линейную систему уравнений. Поскольку линейные системы лежат в основе многих научных и инженерных проблем, потенциальное ускорение, обеспечиваемое алгоритмом HHL, может иметь большое влияние.

Как видно, квантовой угрозе подвержены только конкретные алгоритмы, а не шифрование в целом. Согласно NIST, из применяемых в Америке алгоритмов, квантовой угрозе подвержены AES, SHA-2, SHA-3, RSA, ECDSA, ECDH и DSA. И даже при такой ситуации перспектива расшифрования перехваченных данных специалистами оценивается годами. Специалисты говорят о вероятности один к семи, что алгоритм с открытым ключом будет расшифрован к 2026 году и пятьдесят на пятьдесят, что к 2031.

Самым известным действующим образцом квантового вычислителя пока является компьютер ORION фирмы D-Wave System. В феврале 2007 г. фирма D-Wave System сообщила о создании на основе современной планарной технологии сложной структуры, содержащей 16, а затем и около 50 туннельно связанных флуксоидных сверхпроводниковых ку-битов, которая была представлена как первый шаг к полномасштабному квантовому компьютеру. В настоящее время у потребителей смонтировано 2–3 действующих образца, а максимальное количество ку-битов составляет 2048 штук. Ориентировочная стоимость одного образца составляет 15 миллионов долларов США.

Перспективными направлениями исследований в области квантовой информационной безопасности являются:

- квантовое шифрование;
- квантовая аутентификация;
- квантовая неподатливость (non-malleability);
- квантовое полностью гомоморфное шифрование;
- безопасные многосторонние квантовые вычисления;

- функциональное квантовое шифрование;
- квантовое машинное обучение;
- квантовая генерация случайных чисел.

Рассмотрев технологическую составляющую и существующие алгоритмы квантовых вычислений, вернемся к вопросам квантового и постквантового шифрования. Как было рассмотрено, квантовые компьютеры позволяют проводить вычисления на совершенно иных скоростях, чем современная вычислительная техника, что делает задачу дешифрования зашифрованного текста вполне реальной. Для данных, требующих обеспечения конфиденциальности на срок 10 лет и более, вопрос выбора правильной криптографии стоит наиболее остро и квантовые компьютеры могут стать для таких данных вполне реальной угрозой, к которой надо готовиться уже сейчас.

С точки зрения квантовых вычислений вся криптография может быть разделена на два типа – квантово-безопасная и квантово-небезопасная. К первой относятся многие симметричные алгоритмы (в т.ч. AES или ГОСТ Р 34.12–2015), но с увеличенной как минимум вдвое длиной ключа (какая длина будет достаточной, пока неизвестно). А вот криптоалгоритмы, базирующиеся на сложности факторизации целых чисел (например, RSA) или дискретного логарифмирования (например, Эль-Гамаль или эллиптические кривые), не являются квантово-безопасными.

К ним относятся современные ассиметричные криптографические алгоритмы. Они используют для генерации открытого и закрытого ключей, задачи целочисленной факторизации, которые трудно преодолеть при нынешних вычислительных мощностях.

К примеру, достижения в области квантовых вычислений станут значительными для безопасности блокчейна из-за их влияния на текущую практику криптографии. Например, Биткойн использует криптографические алгоритмы для создания пары открытого и закрытого ключей и адреса, который получается с использованием операций хеширования и контрольной

суммы открытого ключа. Раскрытие одного лишь адреса не является большим риском. Однако раскрытие адреса и открытого ключа, применяемого при транзакции, потенциально опасно т.к. при наличии достаточного прогресса в квантовых вычислениях, позволит получить закрытый ключ. В то время как коммерческие квантовые вычисления недоступны как крупномасштабная реальность, имеет смысл запланировать переход к устойчивой к квантовой криптографии. В настоящее время NIST находится в процессе разработки стандартов квантовой криптографии, а АНБ рекомендует своим поставщикам внедрить SHA-384 вместо SHA-256.

Постквантовая криптография предполагает внедрение новых для современной ИТ отрасли алгоритмов шифрования, которые сложны для взлома как классическими, так и квантовыми компьютерами. Это могут быть как новые, так и ранее известные алгоритмы, применение которых было ограничено ввиду повышенной ресурсоемкости вычислений. Как будет изложено ниже, квантовые вычисления способны решить лишь определенный круг задач с повышенной скоростью. Поэтому не все алгоритмы подвержены квантовой угрозе. Так же следует отметить, что не все квантово-стойкие алгоритмы ресурсоемки. Существуют исследования, подходящие для применения даже в таких областях, как конечные устройства интернета вещей.

Постквантовая криптография — это ответ на квантовые вызовы. Основные усилия в этой области сосредоточены на задачах синтеза стойких к возможностям квантовых компьютеров криптографических алгоритмов и протоколов. Можно выделить четыре направления исследований: криптография на целочисленных решетках, схема электронной подписи Меркля, квантовая схема электронной подписи, аутентификация квантовой информации. Почти все публикации посвящены криптосистемам с открытым ключом и схемам электронной подписи. Недостаточное внимание пока уделяется постквантовым протоколам интерактивной аутентификации, голосования, электронных платежей и т.д. Появление и достаточно быстрое

расширение области исследований, объединенных понятием "постквантовая криптография", свидетельствует о серьезном отношении криптографического мира к проблемам, которые влечет за собой реализация квантовых алгоритмов, и делает целесообразным продолжение исследований как по вопросам квантового криптоанализа, так и по вопросам квантового криптосинтеза.

Постквантовая криптография предполагает, что несмотря на то, что современные квантовые компьютеры еще не внедрены широко, уже сегодня требуется использование новых алгоритмов шифрования способных обеспечить безопасность информации в будущем. Хотя постквантовое шифрование и не использует технологии квантовых вычислений, оно уже сейчас является актуальным средством обеспечения информационной безопасности.

Рассмотрев вопросы постквантовой криптографии, перейдем к тому, как непосредственно квантовые компьютеры могут помочь в обеспечении информационной безопасности. В квантовой криптографии для шифрования используется сложный ключ, который передается от отправителя к получателю посредство элементарных частиц света – фотонов. (Механизм квантового распределения ключей). Защита ключа от перехвата обеспечивается благодаря тому, что даже самый чувствительный прибор неизбежно изменит состояние фотона.

На момент 2016 года существовали десятки различных по назначению протоколов квантовой безопасной связи BB84, ЭПР, B92(4+2), SARG04, CSS, ЛО-ЧУ, Гольденберга-Вайдмана, Коаши-Имото, Пинг-понг и др.

Квантовое распределение ключей, в т.ч. основанное на квантовой телепортации, направлено на защиту ключей шифрования, передаваемых по специализированным, но незащищенным каналам связи. После их применения, информация в зашифрованном виде может передаваться по любым каналам. В настоящий момент применяются сети топологии точка-точка. Создание квантовой памяти и квантовых повторителей пока остается

перспективой дальнейших разработок. В основе теории квантового распределения ключей лежит принцип квантовой неопределенности, в следствии которого, после измерения квантового состояния система возвращается к исходному состоянию. Таким образом перехват ключа злоумышленником в момент передачи сделает невозможным его использование легитимным пользователем, что будет свидетельствовать о постороннем вмешательстве и выявлении атаки в реальном времени. Однако на практике системы не являются идеальными, существуют атаки на суперпозицию (superposition attack), расщепление фотонов (photon number splitting), расщепление потока (beam-splitting), воздействие низких температур (thermal blinding), а также, атаки на конкретные реализации, к примеру на продукты ID Quantique и MagiQ Technologies.

Активные исследования в этой области сегодня проводят компании IBM, ID Quantique, MagiQ Technologies, Nippon Telegraph and Telephone (NTT), QuintessenceLabs, Nucrypt, Oki Electric, Raytheon, Toshiba, Nokia, Fujitsu, Mitsubishi, QinetiQ, и ряд других.

Один из последних продуктов сингапурской лаборатории исследований и разработок в области кибербезопасности NUS-Singtel позволяет обеспечить безопасность высокоскоростной квантовой связи QKD на основе эффективных «коробочных решений».

Последний квантовый процессор Google «Bristlecone» имеет рекорд в 72 кубита с очень низким коэффициентом ошибок и, как ожидается, будет более мощным, чем могут моделировать лучшие классические суперкомпьютеры.

Специалистами из оборонного научно-технического университета и научно-технического университета Китая реализовано спутниковое межконтинентальное квантовое распределение ключей, обеспечивающее теоретически безопасное шифрование информации на расстояниях 7600 км и использовавшееся в качестве основы для защищенной телеконференции между Австрийской академией наук и Китайской академией наук.

Они реализовали квантовое распределение ключей по протоколу decoy-state между спутником на низкой околоземной орбите и несколькими наземными станциями, расположенными в Синлуне, Наньшане и Граце, которые генерируют безопасные ключи спутник-земля с частотой измеряемой в килогерцах при проходе спутника Micius над наземной станцией. Таким образом, спутник устанавливает безопасный ключ между собой и, скажем, Xinglong, и еще один ключ между собой и, скажем, Graz. Затем, по запросу наземной команды, Micius действует как доверенный ретранслятор. Он выполняет побитовые операции исключающего ИЛИ между двумя ключами и передает результат одной из наземных станций. Таким образом, секретный ключ создается между Китаем и Европой в точках, разделенных на 7600 км. Эти ключи затем используются для межконтинентальной квантово-защищенной связи. Была продемонстрирована возможность передачи изображений, с использованием криптосистемы одноразового блокнота, из Китая в Австрию, а также из Австрии в Китай. Кроме того, была проведена видеоконференция между Австрийской академией наук и Китайской академией наук, которая также включала в себя 280-километровую оптическую наземную связь между Синлуном и Пекином.

Австралийская компания QuintessenceLabs совместно с Vault Cloud и Ziroh Labs выпустили безопасный и масштабируемый пакет для корпоративных систем синхронизации файлов и совместного использования файлов в Австралии. Проект предусматривает использование гомоморфного шифрования.

Сингапурская компания ST Engineering совместно с Сингапурским национальным университетом разрабатывают технологию квантового распределения ключей. Целью проекта является создание нового чипа, на базе которого будет разработан квантовый криптографический модуль.

Реализация таких технологий стала возможной благодаря следующим свойствам квантовых систем:

- невозможность произвести измерение квантовой системы, не нарушив ее;
- невозможность определить одновременно координату и состояние частицы со сколько угодно высокой точностью;
- невозможность одновременно проверить поляризацию фотона в вертикально-горизонтальном и в диагональных направлениях;
- невозможность дублировать квантовое состояние, пока оно не измерено.

Несмотря на большой интерес к квантовым коммуникациям, нет абсолютно никакого представления в научном мире о том, как концепция сети будет взаимодействовать с квантовыми вычислениями. Фактически, для квантовых вычислений не существует понятия ни о хранилище, ни о вводе-выводе. Буквально все, что включает технология - это набор ку-битов, которые можно подготовить и измерить, но нет концепции ку-бита или квантовых логических вентилей, обеспечивающих взаимодействие с внешним миром. Дело в том, что настоящая квантовая сеть позволит ку-битам беспрепятственно перемещаться по сети и поддерживать соединение между удаленными квантовыми машинами, однако текущие исследования еще далеки от этого.

Для решения таких задач необходимы квантовые вычислительные устройства, совместимые с устройствами квантовой связи. С одной стороны, лучшая платформа для квантовой коммуникации - фотонная, поскольку квантовую информацию, закодированную в фотонах, просто отправлять на большие расстояния. С другой стороны, один из наиболее многообещающих подходов к устройствам квантовых вычислений, тот, который используется крупными промышленными игроками и возглавляет гонку «больших квантовых компьютеров», основан на сверхпроводящих ку-битах. Предпочтительные типы кубитов для связи и вычислений не совпадают, и, более того, в настоящее время даже не известно, совместимы ли они. Неизвестно, могут ли сверхпроводящие квантовые компьютеры быть частью

«сетевой архитектуры», поскольку в настоящее время они построены в виде монолитной архитектуры, и неясно, будет ли когда-либо возможно отправлять и получать квантовые состояния.

Рассмотрим квантовую криптографию. Специалисты в области квантовой криптографии полагают, что квантовое шифрование может стать перспективным решением для интернет вещей. Квантовые вычисления имеют возможность создавать практически не взламываемые сети устройств и данных, что чрезвычайно актуально для растущего с экспоненциальной скоростью рынка интернет вещей. В частности, швейцарская компания WISeKey представила концепцию использования квантовой криптографии в сетях интернет вещей.

По-мнению аналитиков, глобальный рынок квантовой криптографии к 2026 году может достичь 1 трлн.долларов США.

Еще одним примером является технология потокового шифрования AlphaEta. Принцип шифрования информации базируется на использовании многоуровневого кодирования поляризационных или фазовых степеней свободы когерентных оптических состояний, являющихся в общем случае многофотонными. В 2004 г. была продемонстрирована возможность ее использования с потоком данных в оптоволоконных сетях со спектральным разделением сигналов. Скорость передачи шифрованных данных составляла 155 Мбит/с, квантовый ключ длиной 1 Кбит обновлялся каждые 3 с. AlphaEta также была успешно протестирована на существующей волоконно-оптической линии связи длиной около 850 км. Скорость передачи зашифрованных данных составляла 622 Мбит/с.

Для обеспечения достаточно высокого уровня информационной безопасности, может быть использован открытый инфракрасный луч. Его безопасность является следствием самой природы передач сигнала, а не обеспечивается какими-либо специальными методами. Важнейшее свойство беспроводной оптической связи – высокая степень защищенности канала от несанкционированного доступа. Осуществить перехват канала технически

весьма трудно – в силу острой направленности луча и применения уникального для каждой модели метода кодирования информации импульсами излучения. Тем не менее, для обнаружения попыток несанкционированного доступа разработан ряд мер, основанных на разнообразных принципах – обращения волнового фронта, анализа изменения принимаемого сигнала и др., что еще больше повышает защищенность канала связи.

Не менее важным с точки зрения обеспечения информационной безопасности является инфраструктура классических компьютеров, обеспечивающих работу квантовых. Квантовые компьютеры редки и дорогостоящи. Однако проведение исследований квантовых алгоритмов доступно и без использования такого рода оборудования. Провести тестирование и анализ квантового алгоритма позволяют различные библиотеки симуляции квантовых алгоритмов. Это позволяет найти нужные алгоритмы и затем перенести их на квантовые компьютеры. Также существуют квантовые алгоритмы, в которых оракул можно заранее вычислять на классическом компьютере и затем с его помощью решать более сложные задачи в квантовой модели.

Главная проблема использования квантового алгоритма на классическом компьютере заключается в том, что для работы можно использовать набор входных данных, имеющий только небольшие размеры. Трудность моделирования средних и больших квантовых систем на классических компьютерах обуславливается тем, что количество комплексных чисел, необходимых для описания квантовой системы растет с увеличением размера системы экспоненциально, а не линейно, как для классических систем.

Так же следует отметить, что большинство квантовых систем являются замкнутыми. Конечно, обсуждается квантовый интернет и другие варианты реализации технологии. Но в настоящий момент и обозримом будущем системы останутся закрытыми. Поэтому вопросы обеспечения

информационной безопасности на этапе написания программного кода квантовых цепей остаются теоретическим вопросом. Хотя не следует забывать, что особенности квантового распределения ключей, обусловленные коллапсом волновой функции после измерения ее состояния и невозможности определения волновой функции другими способами, равно как и измерения волновой амплитуды (вероятности) значительно затрудняет отладку уже созданных квантовых цепей постфактум с целью обнаружения уязвимостей и обеспечения защищенности системы. Так же невозможны классические операции мониторинга и журналирования.

Симуляторы позволяют устранить это недостаток, но ограниченность возможностей классического компьютера не позволяют провести симуляцию в полном объеме.

Важным направлением является создание квантовых генераторов случайных чисел, основанных на элементарном оптическом процессе.

Две основные категории классической генерации случайных чисел - это генераторы псевдослучайных чисел и генераторы истинных случайных чисел.

Квантовые генераторы случайных чисел (КГСЧ) можно рассматривать как частный случай истинного генератора случайных чисел, в которых данные являются результатом квантовых событий. Но в отличие от традиционных, квантовые, обещают действительно случайные числа, используя случайность, присущую квантовой физике. Истинный генератор случайных чисел обеспечивает высочайший уровень безопасности, поскольку сгенерированное число невозможно угадать.

В основе этого лежат физические процессы. Фотоны света от источника друг за другом направляются на полупрозрачное зеркало и детектируются двумя приемниками, срабатывание одного из которых ассоциируется с единицей, а другого – с нулем. Построенные по этому принципу КГСЧ со встроенным мониторингом возможных сбоев серийно выпускаются в ряде стран и обладают скоростью генерации до 16 Мбит/с.

Один из КГСЧ был сертифицирован одной из всемирно известных компаний, тестирующих игры для онлайновых игровых приложений.

Samsung и южнокорейский телекоммуникационный гигант SK Telecom представили смартфон Galaxy A Quantum 5G, оснащенный чипсетом с генерацией квантовых случайных чисел (ГСЧ). Это первая коммерциализация квантовой технологии для мобильных телефонов. Чипсет размером 2,5 на 2,5 мм был разработан швейцарской дочерней компанией SK Telecom ID Quantique.

Квантовый чип имеет встроенный светодиодный источник света, который излучает фотоны; он также имеет CMOS-датчик изображения для обнаружения испускаемых фотонов. Датчик изображения отвечает за прием фотонов, а затем за генерацию случайных чисел, используемые в конечном итоге для создания ключей шифрования.

Согласно пресс-релизу, Galaxy будет использовать квантовый ГСЧ в нескольких различных сценариях. К ним относятся вход в учетные записи, надежное хранение личных документов через «Quantum Wallet» с поддержкой блокчейнов, мобильные платежи на основе биометрии в розничных магазинах. В перспективе планируется защита платежей онлайн.

Технологии Роботизированной Автоматизации процессов (РАП)

Цифровизация бизнеса позволяет предприятиям существенно ускорить рабочие процессы и повысить общую производительность при значительном сокращении количества ненужных действий. Цифровые данные становятся все более ценными, поэтому компании должны обеспечить им должную защиту от кибератак, и именно в этой сфере может помочь РАП.

RPA (Robotic Process Automation, РПА, Роботизированная Автоматизация Процессов) — технология, предназначенная для автоматизации процессов, укладывающихся в чёткие алгоритмы. Как

правило, такие процессы связаны с работой с информацией: сбором, консолидацией, поиском, разносом, переносом и т.п.

Ключевой особенностью RPA является возможность роботизировать те процессы, которые иначе автоматизировать было бы невозможно или неоправданно сложно (долго, дорого): там, где отсутствует возможность подключиться по API (Application Program Interface) и классические способы скриптовой интеграции перестают работать. Программный робот может использовать GUI (графический пользовательский интерфейс) и смотреть на экран монитора «как человек», что даёт ему возможность взаимодействовать с элементами на экране. Это актуально для «устаревших» систем, которыми компании пользуются уже десятки лет, а также программ, у которых ограничен или вовсе отсутствует API. Использование настраиваемых программных роботов, имитирующих действия человека по взаимодействию с информационной системой, позволяет автоматизировать различные процессы так, что система не видит разницы между роботом и человеком

В российских условиях RPA может найти достаточно широкое распространение в кибербезопасности, т.к. многие отечественные решения не имеют API и не умеют взаимодействовать между собой

Роботы могут работать с Web-формами, приложениями, почтой, документами, базами данных, файлами на диске или в Интернет, которые могут быть преобразованы по заданному сценарию или алгоритму.

RPA хорошо работает в совокупности с другими инновационными решениями так называемой Индустрии 4.0, в частности с Машинным Обучением (Machine Learning) и Оптическим Распознаванием Символов (OCR, Optical Character Recognition). При подключении OCR программный робот RPA может получать информацию из любых документов, будь то паспорт или акт выполненных работ, в неструктурированном виде, а затем, следуя своему алгоритму, заносить необходимые данные в информационные системы компании. А при подключении модуля машинного обучения, основываясь на большом количестве данных за предыдущее время,

прогнозировать и принимать взвешенные решения, например, по степени риска, или подбирать информацию для заполнения соответствующей ячейки в системе.

Работает с любыми программными продуктами, например: 1С, SAP, Bitrix, АБС, приложения Microsoft и т.д.;

Оптимизируют производственные и человеческие ресурсы, люди заняты важной и интересной работой с большей добавленной стоимостью;

Повышается скорость выполнения автоматизированного процесса, а также смежных процессов, зависящих от него;

Исключаются ошибки из-за усталости или невнимательности, точность выполнения алгоритма 100%;

Короткий цикл внедрения, в среднем занимающий около 2 месяцев;

Не требует внесения каких-либо доработок в текущую ИТ-структуру, робот встраивается в неё (или поверх неё);

Средний срок окупаемости роботизации около 7 месяцев.

При внедрении робота от 2-х дней занимает изучение процесса, определение необходимых приложений и ИС, с которыми нужно работать, и снятие скриншотов действий пользователя. От 5-ти дней уходит на настройку робота - сценариев его работы и взаимодействия с нужными системами. От 3-х дней уходит на тестирование и доработку робота. Для простых случаев автоматизации внедрение робота занимает около 10 дней - в более сложных может понадобиться 1-2 месяца.

К примеру, будучи установленным на компьютере пользователя или на сервере, робот сам, через заданные интервалы может выгружать журналы регистрации из облачной платформы и преобразовывать в нужный формат и передавать в SIEM. Ту же задачу можно было бы возложить на скрипт, написанный на каком-либо языке программирования, но только при условии, что есть специалист, способный реализовать это и облако поддерживает API, который можно вызывать из скрипта. В противном случае задача может потребовать дополнительных ресурсов. Робот не требует ни знаний

программирования, ни наличия API. С помощью визуального конструктора (схожая идея реализуется в различных SOAR) описываются действия, ответы систем и их интерпретацию.

Другим примером может служить следующий набор операций:

- заход в личный кабинет ФинЦЕРТ или ГосСОПКА для получения бюллетеней или уведомлений;
- обогащение событий безопасности из источников TI;
- заведение тикетов в IRP / SOAR;
- анализ заявок на предоставление доступа к корпоративным ресурсам;
- организация фишинговых симуляций
- сбор облачных логов в Excel/CSV и загрузка их в SIEM
- анализ входящих сообщений от пользователей
- работа с унаследованными или legacy системами ИБ
- тестирование защищенности Web-приложений
- сбор инвентаризационных данных из десятка источников и приведение к единому формату с загрузкой в CMDB
- мониторинг Интернет-ресурсов, а также анализ новостей по ИБ и отправка ключевых во внутреннюю рассылку
- построение dashboard
- получение согласий на обработку ПДн от клиентов;
- уведомление о нарушении прав субъекта ПДн.

Это неполный перечень, но он достаточно показательный. С помощью RPA можно автоматизировать многие рутинные задачи, возникающие в деятельности ИБ.

Одним из направлений использования РАП в интересах информационной безопасности является создание ботов, предотвращающих при появлении предупреждения от антивирусной системы использование соответствующих файлов.

Встроенные в корпоративную систему боты могут выполнять рутинную работу по соблюдению нормативных требований, таких как резервное копирование, ведение различных реестров и протоколов.

РАП активно используется для ограничения доступа неавторизованных пользователей к информации. Безопасный доступ необходим для защиты предприятий от случайных ошибок сотрудников, а также от сложных хакерских атак. В случае необходимости РАП может создать дополнительный уровень шифрования для более безопасного использования данных.

Наиболее ценным качеством РАП является возможность снизить риск непреднамеренных ошибок, вызванных «человеческим фактором». Например, при заполнении электронных таблиц или из-за необходимости отключения слишком большого количества приложений при завершении работы.

Когнитивные способности RPA роботов и искусственный интеллект в совокупности предоставляют ряд преимуществ для предотвращения подобных ошибок, повышая продуктивность сотрудников, а также является более дешёвой альтернативой. Если с чувствительной или конфиденциальной информацией работают живые люди, существует риск целенаправленной кражи данных или её случайного разглашения из-за халатности. В отличие от человека, роботы с поддержкой ИИ выполняют исключительно те операции, которые в них заложены, но они также могут учиться во время выполнения самого процесса, а затем передавать эти знание другим ботам.

Выполняя рутинные, но необходимые нормативные операции, РАП позволяют сотрудникам высокой квалификации сосредоточиться на более сложных важных задачах.

Искусственный интеллект при поддержке RPA-робота может поднять уровень аварийной готовности на совершенно другой уровень. RPA – идеальная технология для соблюдения GDPR и прочих регулирований,

гарантирующих и защищающих бесперебойный доступ к информации. RPA также может делать бэкапы ключевых процессов в случае необходимости выключения или перезапуска всей системы. RPA быстро сохраняет информацию и получает её из офлайн источников, что позволяет держать информацию «под замком».

Автоматизация анализа записей в контрольном журнале может существенно усилить внутренний контроль в банках или других индустриях, для которых важна точность.

RPA робот может осуществлять операции с малыми и большими объёмами данных на границе разделенных сетевых сегментов, когда информация перемещается из одного места в другое, например, из внутренней ИС на веб-портал или стороннее приложение.

Технология RPA также прекрасно подходит для предотвращения несанкционированного доступа к частной информации. Безопасный доступ необходим для бизнеса как в случае предотвращения случайной утечки информации со стороны сотрудников, так и защиты от хакерских атак.

Построение Центра Компетенций RPA позволит с помощью опытной команды постоянно мониторить задачи, проверять окружение на наличие вредоносного ПО, а также соблюдение политик безопасности компании.

На сегодняшний день в силу активного развития интернета как средства передачи и получения информации остро стоит проблема поиска оптимальных инструментов для обработки и анализа неструктурированных данных.

Неформально проблему можно описать следующим образом. Существует некий набор разнородной информации, из которой необходимо вычленить опорные закономерности, на основании которых можно будет сделать те или иные выводы. Для наиболее эффективного анализа к каждому конкретному типу данных (текстовая информация, изображения, аудио- и видеоинформация) предпочтительно применять специализированные методы, дающие наилучшие результаты и, зачастую, не являющиеся

универсальными. Таким образом, первоочередной задачей становится задача классификации данных. Решение описанной проблемы также возможно с применением технологии Robotic Process Automation (RPA), ориентированной на автоматизацию с использованием программных роботов и искусственного интеллекта, что позволяет эффективно осуществлять сбор и рутинную обработку информации.

PIX RPA Platform – это платформа роботизированной автоматизации процессов, разработанная российской командой PIX Robotics. В команду вошли опытные разработчики и бизнес-консультанты, успешно выполнивших десятки проектов по роботизации на разных RPA-платформах. Аккумулированный опыт был использован для того, чтобы учесть сильные и слабые стороны мировых лидеров и создать продукт, достойный соперничать с передовыми вендорами по роботизации. Встроенная интеграция с продуктами компании "1С" – know-how на рынке продуктов RPA; Автоматизация действий в любых приложениях, встроенный рекордер, работа с OCR "из коробки"; Проект обладает статусом участника Инновационного Центра Сколково.

Digital Workforce Platform – это продукт, предлагающий самообучающихся ботов (IQ Bot), которые совершенствуются, наблюдая (собирая статистику) за действиями человека. Продукт, предлагающий мгновенную аналитику процессов благодаря самообучающимся ботам. Совершенно простой в управлении, доступный любому сотруднику компании с самыми передовыми функциями безопасности.

Automation Anywhere – глобальный лидер продуктов роботизации, компания, ведущая свою деятельность с 2003 года. Головной офис компании находится в г. Сан-Хосе, Калифорния, США. Флагманским продуктом компании является Digital Workforce Platform. Продуктами Automation Anywhere пользуются такие компании, как Google, GM, Siemens, Cisco, Dell, Mastercard, Comcast, а также другие организации из рейтинга Fortune 500.

UiPath взаимодействует с другими ИТ-системами через пользовательский интерфейс, имитируя работу конечного пользователя, в отличие от традиционных компьютерных программ, которые работают через API (Application Programming Interface) или интеграционную шину (Middleware). Решение UiPath Platform позволяет роботизировать практически любые действия пользователя на компьютере.

Интернет вещей

Умный дом позволяет многое сделать с автоматизацией различных сервисов и процессов, в том числе тех, что включены в домашние системы безопасности. Сюда относятся умные дверные звонки, умные замки, умные камеры, умные термостаты, умные лампы и умные пожарные сигнализации.

Крупнейшие компании в области информационных технологий разработали собственные решения для управления интернет вещами, в том числе в целях обеспечения безопасности. Среди наиболее известных следует назвать Google Smart Home, Amazon Echo, Amazon Alexa, Apple Siri и целый ряд других.

Непосредственно в целях безопасности разработаны целая серия различных устройств, позволяющих контролировать и управлять всем комплексом интернет вещей.

ADT Pulse - это подключаемый модуль, который позволяет владельцам дома или офиса управлять системами безопасности и просматривать состояния датчиков. Их API использует функционирующий в импульсном режиме веб-портал компании ADT. В случаи обнаружения одним из датчиков движения внутри помещения или открытия дверей или окон, сигнал от них поступает на портал и далее передаётся на мобильное устройство владельцу помещения.

Устройство Vivint Smart Home - это беспроводная система домашней безопасности. Это многофункциональное, профессионально установленное устройство IoT. В этом устройстве реализована современная концепция DIY,

упрощающая процесс инсталяции и управления системой. Сигнальное оборудование интегрировано с устройствами интернет вещей, включая видеодомофоны и камеры, для управления компактной внутренней системой безопасности.

Аналогичные функции реализованы в устройствах Simpli-Safe, Wink Lookout, Abode-Iota и других.

Большие данные

Считается, что использование технологий больших данных (БД) является настоящим технологическим прорывом в области информационной безопасности.

Основным применением БД в информационной безопасности можно считать технологии мониторинга и обнаружения угроз ИБ. По сравнению с традиционной системой безопасности, технология больших данных, позволяет обнаружить угрозу более эффективно. Например: технология больших данных может обнаруживать ненормальное поведение в сети, прогнозировать поведение атаки и анализировать источник атаки. Анализируя электронную почту, информацию из социальных сетей, можно анализировать и выявлять неудовлетворенных сотрудников на предприятии и своевременно планировать меры по предотвращению нарушений безопасности. Методики анализа безопасности с использованием больших данных обладают следующими характеристиками:

- большие данные хорошо подходят для анализа безопасности - основной технологией анализа безопасности является поведенческий анализ и выявление инцидентов безопасности, это реализуется путем анализа журнала событий и других неструктурированных данных. Большие данные применяются для сбора, хранения и анализа данных журнала. Результат анализа очень важен для защиты и может быть визуализирован.

- спектр анализа контента стал шире - система мониторинга безопасности с использованием технологии больших данных может собирать данные социальных сетей, личную информацию, отслеживать информацию о поездках и вождении, финансовую информацию, заявки в службу поддержки, информацию электронной почты, информацию о покупках, медицинскую информацию, корпоративную деловую информацию. Согласно этой информации, можно проанализировать некоторые аномальные инциденты, связанные с безопасностью, и принять меры противодействия.
- период анализа стал больше - анализ инцидентов безопасности, как правило, занимает очень длительный период времени, он требует больших вычислительных мощностей и большого количества данных. Традиционная система анализа угроз может не отвечать необходимым требованиям, но система анализа угроз, использующая большие данные, может имеет переменный пул ресурсов и может анализировать огромные объемы данных, чтобы как можно скорее предсказать инциденты безопасности, такие как APT-атака.
- необходимость предсказывать и прогнозировать угрозы - традиционная система анализа угроз имеет в своем распоряжении небольшой объем данных, небольшой диапазон, короткий промежуток времени и не может предсказать инциденты безопасности на основе картины в длительной ретроспективе. Система анализа угроз, использующая технологию больших данных, может прогнозировать надвигающуюся угрозу используя множественные характеристики.
- обнаружение неизвестных инцидентов - основываясь на историческом опыте, мы можем обнаруживать инциденты безопасности, произошедшие раньше, но мир постоянно меняется и могут возникать новые инциденты безопасности, угрозы нулевого дня. Аналитическая работа в традиционной системе выполняется опытными аналитиками или продвинутыми алгоритмами, но они в основном выносят суждения на основе событий, увиденных ранее, поэтому они не могут обнаружить неизвестный

инцидент. Инциденты безопасности часто взаимосвязаны, система анализа угроз, использующая технологию больших данных, может обнаруживать неизвестные инциденты безопасности проводя корреляцию между ними, а не опираться только лишь на причинно-следственную связь.

В настоящее время средства обнаружения, предупреждения и предотвращения компьютерных атак и вредоносной активности, а также мониторинга и управления безопасностью представлены различными классами решений. Двумя такими классами являются системы SIEM (Security Information and Event Management) и SOAR (Security orchestration, automation and response).

Основными задачами таких систем являются сбор больших массивов гетерогенных данных о событиях безопасности и обнаружение инцидентов и угроз безопасности в результате их обработки. При этом одной из достаточной острых проблем, стоящих перед современными SIEM-системами, является проблема обработки больших данных, которая вызвана необходимостью обработки огромных массивов разнородных данных о событиях безопасности (логов), поступающих в SIEM-систему от различных источников. В качестве источников больших данных выступают операционные системы, системы управления базами данных, антивирусные средства, сетевые элементы, системы обнаружения атак и т.д.

Современная компьютерная сеть, безопасность которой управляется SOAR-системой, может содержать несколько сотен / тысяч таких источников данных. В результате в SIEM-систему за день могут поступать на обработку данные о десятках / сотнях миллионов событий безопасности. Обработка этих данных включает такие операции, как фильтрация, агрегация, приоритезация, корреляция и другие.

Наибольшей вычислительной сложностью обладает операция корреляции событий безопасности. Суть этой операции заключается в определении причинно-следственных связей между поступающими на обработку событиями. Это позволяет выявлять вредоносную и аномальную

активности, определять источник и цель атаки, обнаруживать многошаговые атаки, делать выводы об инцидентах безопасности и вырабатывать эффективные контрмеры. При этом следует отметить, что все эти действия должны выполняться в реальном или близком к реальному времени, чтобы не дать возможности злоумышленнику реализовать свои вредоносные цели.

Однако проблема выполнения операции корреляции событий безопасности в SIEM системах в реальном или близком к реальному времени остается сложно решаемой проблемой. Ее решение возможно только с использованием современных подходов средств и методов обработки больших данных. Одним из таких подходов является использование современных программных средств реализации параллельных потоковых вычислений. Известно несколько средств реализации параллельных вычислений. К числу наиболее распространенных относятся Hadoop, Spark, Elastic Stack. При этом Spark на больших объемах входных данных показывает более высокую производительность. В то же время Spark является более молодым средством.

Задачей информационной безопасности в области больших данных является формализация задач и реализация алгоритмов выявления связей между типами событий безопасности и оценки зависимости силы связей от распределения событий во времени, решаемых в SIEM-системах при корреляции событий безопасности.

Одним из примеров, является работа по реализации в среде параллельных вычислений различных подходов к выявлению косвенных связей между типами событий безопасности и оценке зависимости силы связи по отношению к времени, основанной на использовании коэффициентов корреляции Пирсона.

Работа развивает методы корреляции, которые позволяют выявлять однотипные и разнотипные связи между событиями безопасности, а также развитии технологии обработки Больших данных на примере корреляции

больших массивов разнородных данных о событиях безопасности в SIEM системах.

О процессе корреляции данных о событиях безопасности принято говорить в широком и узком смысле слова. В широком смысле слова под корреляцией данных понимается вся предварительная обработка данных, собираемых SIEM системой от источников. Результаты этой обработки помещаются в хранилище данных SIEM системы и используются в дальнейшем для проведения более детального и тщательного анализа информации о безопасности.

Обычно в рамках корреляции данных о событиях безопасности, понимаемой в широком смысле слова, выделяются следующие этапы: нормализация (приведение собираемых данных к единому формату); анонимизация (преобразование данных с целью исключения их нежелательного разглашения); фильтрация (отсеивание дублируемых, малозначительных или бесполезных данных); агрегация (получение новых данных с использованием различных функций агрегирования, таких как average(), count(), min(), max() and so on); анализ (нахождение закономерностей появления и зависимостей, в том числе скрытых, между событиями безопасности); собственно корреляция (определение взаимосвязей между экземплярами событий и их групп); ранжирование (оценка результатов корреляции по определенным признакам); приоритезация (вычисление степени важности результатов процесса корреляции). В последовательности этапов, корреляция понимается в узком смысле слова. Ее суть заключается в нахождении причинно-следственных связей между анализируемыми событиями безопасности. Эта операция по своей вычислительной сложности является наиболее сложной из всех перечисленных этапов. Реализация этого этапа с помощью параллельных вычислений представляет несомненный интерес с научной и практической точек зрения.

При проведении вычислений корреляции, входными (исходными) данными является поток данных о событиях безопасности, которые относятся к различным типам. На стадии вычислений происходит обработка входного потока данных, позволяющий выявлять прямые и косвенные связи между экземплярами событий различных типов и допускающий свое распараллеливание.

Различные методы корреляции данных были впервые использованы в Intrusion Detection Systems (IDSs) для обнаружения связей между сетевыми событиями с целью их последующей агрегации и выявления атак, в том числе распределенных и многошаговых. Методы корреляции данных о событиях безопасности, реализованные в IDSs, были в дальнейшем внедрены и адаптированы в SIEM-системах для обработки данных о событиях безопасности.

В настоящее время процесс корреляции данных в различных SIEM-системах отличается большим многообразием реализованных в них методов и подходов. В общем случае следует считать, что для корреляции возможно использование комбинации различных методов, каждый из которых обладает своими достоинствами и недостатками. Все методы корреляции данных можно условно разделить на сигнатурные и эвристические. Данные методы могут применять различные подходы, основанные на анализе схожести, статистическом анализе, интеллектуальном анализе данных и прочие. Анализ применяемых методов корреляции в существующих решениях значительно усложняется ввиду отсутствия работ с детальным описанием используемых методов корреляции.

В настоящее время наиболее распространенным и простым в реализации, однако достаточно сложным в настройке и не приспособленным к автоматизированной адаптации, является правило-ориентированный метод. Основным принципом настройки SIEM-систем, использующих данный метод, является составление правил корреляции в зависимости от характеристик анализируемой инфраструктуры. Работа модуля корреляции

на основе правило-ориентированного метода базируется на фиксированном соотнесении событий друг с другом при выполнении определенных условий. Данные условия могут содержать логические операции над данными, их свойствами и вычисляемыми показателями. Главным недостатком данного метода является сложность процесса составления правил. Другим недостатком является тот факт, что качество выполнения корреляции правило-ориентированным методом напрямую зависит от квалификации администратора безопасности (проектировщика).

Другие методы корреляции, такие как шаблонно-ориентированный (сценарно-ориентированный), граф-ориентированный, основанный на машине конечных состояний, основанный на анализе схожести и другие, по своей сути имеют различные модели представления событий безопасности и их связей. Однако, в конечном итоге, они также могут быть выражены в виде правил, поскольку все они являются сигнатурными методами.

Достаточно интересным современным направлением развития методов корреляции событий является применение подходов, базирующихся на машинном обучении и интеллектуальном анализе данных, таких как байесовские сети, иммунные сети, искусственные нейронные сети и другие. Достоинство данных подходов заключается в возможности самостоятельной (безусловной) корреляции событий с минимизацией ручной настройки. Однако для построения моделей обучения требуется предварительный анализ самих данных, который далеко не всегда можно автоматизировать. Кроме того, применение интеллектуальных подходов накладывает дополнительные требования по оценке адекватности и качества моделей, а исходные данные обучения должны быть репрезентативными.

Применение параметрических и непараметрических показателей корреляции (линейных, различных ранговых и других), в том числе коэффициентов Пирсона, возможно для решения задач оценки алгоритмов, выявления образов распределенных DoS-атак, выделения подмножеств признаков данных, по которым производится обнаружение вторжений на

разных этапах развертывания системы, в том числе, на начальном этапе, когда модели ИИ еще недостаточно обучены и адаптированы к новой среде, для верификации полученных выводов и на стадии применения для интерпретации результатов.

Существуют разные подходы, рассматривается детерминированный и стохастический подходы корреляции событий для задачи обнаружения сетевых атак. Вероятностная модель процесса корреляции событий основана на их пространственно-временном анализе. Пространства событий связываются в цепи последовательностей, а каждому пространству в текущий момент соответствует конкретное состояние из множества состояний. Полученные цепи последовательностей используются для вычисления вероятности выполнения определенного сценария атаки.

Для обнаружения атак в облачной вычислительной среде, можно применить подход корреляции событий в системе распределенных сенсоров Для выполнения подхода предлагается использовать технологию CEP (Complex Event Processing). Онтологическая модель обнаружения атак включает сценарии, индикаторы, симптомы и воздействия атак, а также состояние предполагаемой цели.

Возможно использование модели поведения приложений для выявления неправомерной и аномальной активности. Исходными данными для построения модели являются события, отражающие системные вызовы всевозможных приложений. Выделяют 5 уровней представления модели, верхним уровнем является выделенная функциональность. На основе исходной информации формируется профиль нормального поведения за счет обработки мульти-графа, в котором каждой вершиной является событие.

Для применения современных средства параллельной обработки в процессе корреляции данных о событиях безопасности можно рассмотреть технологии обработки больших данных такие как Stream Processing Engine. Предлагаемый подход позволяет обеспечить гибкое управление ресурсами и балансировку нагрузки с низкими накладными расходами.

Были проведены исследования различных средств обработки больших данных из состава фрэймворков Hadoop и Spark, которые применялись для решения задач анализа сетевого трафика с целью выявления аномальной активности. Для проведения экспериментов был использован вычислительный кластер, а задачи анализа трафика были реализованы за счет самообучающихся алгоритмов. Результаты проведенных исследований показали явное преимущество технологии многопоточной обработки данных Spark над другими продуктами для работы с большими данными. Были выявлены преимущества в точности классификации сетевого трафика с помощью алгоритма случайного леса деревьев решений (Random Forest) над алгоритмом наивного Байеса (Naïve Bayes).

Алгоритмы интеллектуального анализа больших данных для выполнения задач мониторинга безопасности были реализованы в библиотеке MLib из состава фрэймворка многопоточной обработки информации Spark.

Среди современных средств, реализующих параллельные вычисления, одним из наиболее предпочтительных является фреймворк Spark. Необходимо делать акцент на выявлении связей между типами событий и оценке зависимости силы связей от распределения событий во времени. Одним из подходов к оценке указанной зависимости является применение двумерного линейного коэффициента Пирсона, поскольку данный показатель требует наименьших затрат вычислительных ресурсов.

Анализ релевантных работ показывает, что в настоящее время разработано достаточно большое количество методов корреляции данных, которые обладают различными достоинствами и недостатками. Ряд предлагаемых подходов базируется на использовании сценариев атак для формирования последовательностей атакующих действий, что относит их к классу сигнатурных методов и предполагает значительные временные затраты для настройки и адаптации к целевой инфраструктуре. Важным направлением дальнейшего совершенствования методов корреляции является

их адаптация к технологиям обработки больших данных и параллельных вычислений.

Таким образом, технологии БД позволяют в режиме реального времени выявлять новые инциденты и в сочетании с историческими данными прогнозировать подозрительную активность. Наличие большого количества исторических данных значительно упрощает первоначальную калибровку для нормальных моделей активности данной сети. В последующем эти данные используются для выявления различного рода аномалий.

Аналитика БД позволяет отфильтровывать статистический шум, кратно сокращая и классифицируя информацию об инцидентах. Исходная информация сохраняется для последующего анализа и может использоваться экспертами для более подробного анализа.

Перечисленные выше функции нашли свое применение в различных по масштабам использования продуктах.

BM QRadar - решение для крупных предприятий, которым необходимо осуществлять постоянный мониторинг корпоративной информационной системы. Платформа использует распределенную систему SIEM, обеспечивающую горизонтальное масштабирование хранения данных в отдельных узлах. Благодаря такому решению платформа IBM QRadar проста в управлении и экономична.

RSA Security Analytics - предоставляет дополнительные сведения о сетевых сеансах путем анализа сетевого трафика. Полученная информация позволяет специалистам в области информационной безопасности более глубоко анализировать весь комплекс возникающих проблем.

LogRhythm - решение для анализа БД, поддерживающее различные типы данных: информацию об инцидентах, системные журналы, журналы аудита, журналы приложений информацию об активности процессов, целостности файлов, поведении пользователей.

Splunk Enterprise Security - позволяет аналитикам выявлять вредоносные инструменты и собирать данные в контексте этих событий, используя визуализацию анализа данных.

Голландский институт Netherlands Forensic Institute разработал программно-аппаратный комплекс Kesida. Аналитические инструменты комплекса позволяют базируясь на больших данных поводить цифровые расследования и выявлять нарушения в различных областях жизнедеятельности

AdaptiveDefense – это новый продукт Panda, который ориентирован на противодействие угрозам повышенной сложности (APT) и новому поколению вредоносных программ, с которыми традиционные антивирусные решения могут не справится. Данный продукт представляет собой прекрасный пример того, насколько успешно и эффективно используются большие данные и машинное обучение в инструментах безопасности.

AdaptiveDefense способен в реальном времени непрерывно анализировать поведение всех программ, которые пытаются запуститься в системе, автоматически классифицируя все приложения благодаря алгоритмам машинного обучения. Это позволяет пользователю получать немедленные оповещения с детальной информацией, объясняющей природу и активность вредоносных программ, и даже активировать такие режимы блокировки, при которых возможен запуск только программ, классифицированных как goodware (невредоносные программы).

Подводя итог, необходимо упомянуть, что рассмотренное применение технологии не является единственным. К примеру, БД могут использоваться как технология аутентификации личности по характеристикам поведения. Традиционные технологии аутентификации основываются на трех способах: кто я (биометрическая аутентификация), что я знаю (аутентификация по паролю), что у меня есть (ID-карта). В среде больших данных пользователи могут быть аутентифицированы по поведенческим характеристикам.

Это отличается от принятой концепции аутентификации, однако установлено, что пользователю сложно пройти аутентификацию путем подделки модели поведения. Применение такого подхода может уменьшить нагрузку на пользователя, пользователю не нужно помнить сложный пароль или идентификационную карту, либо служить дополнительной мерой по усилению защиты.

Заключение

Американская аналитическая компания Гартнер поставила проблему кибербезопасности в 2020 году на первое место. Актуальность этой проблемы заставляет правительственные органы и корпорации уделять повышенное внимание развитию технологий информационной безопасности. Приведенные выше примеры использования отдельных «сквозных» технологий иллюстрируют их высокий потенциал для решения важнейших задач по совершенствованию и развитию отрасли информационной безопасности.