**Охрана предприятия**

**№4 (80), 2021**

**Оглавление**

# Распространенные ошибки в резюме соискателей на топ должности в охранной индустрии

Журнал Chief Security Magazine, July 15, 2021, опираясь на мнения экспертов, разбирает наиболее часто встречающиеся ошибки в резюме кандидатов на ведущие позиции в сфере охраны и корпоративной безопасности.

*Отсутствие указаний на лидерские компетенции*

Как считает Ник Джайнас из консалтинговой компании WittKieffer, многие соискатели при подготовке резюме опускают информацию, которая бы демонстрировала лидерские качества. Например, такие как:

- своевременное обнаружение и анализ изменений в ландшафте угроз и рисков;

- приоритетное внимание информированию первых лиц в компании о текущих и прогнозируемых рисках;

- умение налаживать и поддерживать взаимодействие с правлением и руководителями других подразделений;

- подготовка, обучение и карьерное продвижение молодых кадров.

Очень часто резюме не позволяет оценить способность кандидата формировать видение перспектив компании, разрабатывать и осуществлять стратегию управления рисками.

*Невнимание к реальным своим достижениям*

Соискатели нередко забывают включать в резюме информацию об объеме и задачах работы, которую они выполняли на прежних должностях, о численности команды, которую возглавляли. Как замечает Брандон Парезо из рекрутинговой фирмы LaSalle Network, «они не пишут, чему учились и как приобретали компетенции руководителя на прежней работе».

*Слишком большой упор на технологические знания*

Этот недостаток касается, прежде всего, менеджеров по кибербезопасности, претендующих на место руководителя отдела информзащиты. Безусловно, техническая квалификация здесь – приоритетна. Но она не предполагает обязательного насыщения текста резюме малопонятными не специалисту терминами, сокращениями, жаргонными словечками. Этим грешат многие профессионалы в

области кибербезопасности. Говорит Парезо: «О своих технологических компетенциях надо рассказывать языком бизнеса. Не разбирать эффективность того или иного проекта информационной защиты, но показывать собственную лидерскую роль в его осуществлении, и как этот проект помог развитию бизнеса».

При этом не надо скрывать факты инцидентов безопасности, в частности, успешных хакерских атак, с которыми сталкивались соискатели. В этой части резюме важно рассказать, как вы справлялись с проблемой, чему научились, что сделали для укрепления безопасности.

*Игнорирование опыта внутри и межотраслевых связей и контактов*

Работодатели в лице акционеров и управляющих бизнесом хотят, чтобы их топ-менеджеры были достаточно активными в отраслевых ассоциациях на региональном и даже национальном уровне. Им надо быть уверенными, что приходящие в компанию менеджеры будут всегда в курсе зарождающихся тенденций и новых стратегий в своем профессиональном сегменте.

С другой стороны, не надо уж слишком акцентировать внимание на своем участии в конференциях, форумах, чатах, что может создать впечатление о приоритетном стремлении делать себе имя в ущерб должностным обязанностям. Как всегда и везде, нужен верный баланс.

*Слабое форматирование резюме, школьные ошибки, ненамеренные искажения*

Несмотря на гигантское развитие Интернета, социальных сетей, поисковых машин резюме по-прежнему придают большое значение. Участвующие в отборе кандидатов изучают его внимательнейшим образом. И, конечно, обращают внимание на опечатки, если их много, отсутствие контактных и прочих важных данных, слабое форматирование.

Эксперты настоятельно рекомендуют обращать внимание на такие базовые правила составления резюме как его размер, формат и точность. Объем не должен превышать нескольких страниц. На первом месте – лидерские компетенции и ориентация на бизнес. Технические знания, профессиональное признание, детали обучения – на втором.

# Искусственный интеллект в системах охраны школ

Широкие дискуссии о том, как обезопасить школьников и учителей от стрелков-террористов обычно сводят проблему к набору известных средств - металлодетекторам, вооруженным охранникам, специальным тренингам, пуленепробиваемым окнам и дверям…

Между тем, исследования, проводимые в разных странах, показывают, что наиболее эффективным инструментом безопасности учебных заведений (и не только учебных) является информация, позволяющая предотвратить потенциальную угрозу. Речь идет,

прежде всего, о том, что по понятным морально-психологическим причинам нередко вызывает у нас неприятные ассоциации и ощущения, а именно - о поощрении добровольного доносительства по поводу подозрительного поведения тех или иных учащихся.

Создание информационной системы предупреждения, как и любое другое дело, невозможно без внимания к трем ключевым моментам: участникам, процессам и технологиям. Что касается последних, то, по мнению Питера Эванса, автора статьи в журнале Security Magazine, August, 2021, наиболее перспективными и востребованными являются инновации в области искусственного интеллекта. Эванс называет четыре зоны для практического применения ИИ в охранном деле.

1. В онлайне

Идеальное решение – обнаружить и остановить потенциального преступника (здесь: ученика или выпускника) до того, как он/она переступит черту, за которой следует правонарушение. Подростки, вынашивающие планы мести одноклассникам или учителям, нередко делятся своими чувствами и переживаниями в социальных сетях. Программные приложения на базе искусственного интеллекта способны в процессе онлайнового мониторинга электронной переписки, интернет чатов и форумов идентифицировать признаки потенциальной угрозы насилия и передавать соответствующую информацию администрации школы и в правоохранительные органы.

2. Вне здания, на территории, прилегающей к школе

Во многих американских школах, пишет автор публикации, уже установлены системы наружного видеонаблюдения, покрывающие паркинг и прочие зоны вокруг школы. Их усиление технологией ИИ существенно расширяет возможности своевременного информирования об оружии, насилии или подозрительном поведении учащихся вне стен школы, например, о возникшей рядом со школой драке.

3. На входе в здание

В большинстве школ сегодня количество подъездов сведено к минимуму. Они охраняются, в том числе, и металлодетекторами. Мера необходимая, но порождающая другую проблему – скученность, толкотню перед занятиями, на переменах, после уроков. Вооруженные искусственным интеллектом системы СКУД представляют собой эффективную альтернативу металлодетекторам, поскольку они запрограммированы на обнаружение только холодного и огнестрельного оружия, а не всех подряд металлических предметов. Тем самым, решается проблема очередей.

4. Внутри здания

И здесь искусственный интеллект, интегрированный в систему внутреннего видеонаблюдения, незаменим для своевременного обнаружения оружия или другого запрещенного в школе предмета, пишет Эванс. В том случае, если «активный стрелок» уже проник в школу, камеры наблюдения предоставят полиции в режиме реального времени детальную картину маршрута движения стрелка и его действий.

Кроме террористической угрозы администрация школы с помощью ИИ может отслеживать нежелательные акции и поведение учащихся (потасовки, вандализм, курение), а также, например, контролировать, все ли двери закрыты.

Конечно, заключает автор статьи, искусственный интеллект не решает все проблемы, связанные с охраной здоровья и жизни учащихся и учителей, но делает работу по безопасности намного эффективнее. С точки зрения финансовых затрат, использование технологий ИИ не требует огромных дополнительных инвестиций. Соответствующие приложения и программы во многих случаях адаптируются к уже имеющейся в школах компьютерной инфраструктуре.

# Биометрическая идентификация по поведенческим характеристикам

Пандемия коронавируса вызвала взрывной рост дистанционных форм работы. Массовое распространение т.н. «удаленки», в свою очередь, привело к деформации традиционных инфраструктур многих компаний и организаций, чем воспользовались хакеры и мошенники, эксплуатирующие новые уязвимости в системах информационной защиты.

«Каждое домашнее соединение с корпоративной сетью, не будучи надлежащим образом защищено, представляет собой потенциальную цель для атаки», пишет Леандро Маргулис в онлайновом издании Security Magazine, August, 2021. Новая реальность настоятельно требует дополнительных защитных механизмов, которые бы гарантировали безопасность компании от киберкриминала. Ответом на возросшие угрозы являются двухфакторная и многофакторная виды идентификации.

Усложненные виды идентификации, с одной стороны, усиливают защиту, но, с другой – добавляют пользователям неудобства. Некоторые компании предпочитают «оптимизацию», т.е. облегчать клиентам и сотрудникам доступ к корпоративной информации за счет безопасности. Но это ошибочный путь, считает Моргулис, особенно в условиях, когда подавляющее число финансовых трансакций осуществляется цифровым способом.

Бизнесу проще заставить своих работников следовать многофакторной идентификации, чем накладывать такие же обязательства на клиентов, партнеров, потребителей продуктов/услуг. В последнем случае всегда присутствует риск, что из-за дополнительных сложностей клиенты просто побегут к конкурентам, придерживающихся традиционной, облегченной конфигурации контроля за допуском.

Как же совместить удобство и безопасность без ущерба для компании и пользователей?

Автор публикации обращает внимание на биометрию как технологию, которая позволяет идентифицировать и верифицировать личность на основе одной или нескольких физиологических статических характеристик, присущих исключительно одному человеку (отпечатки пальцев, очертание лица, радужная оболочка глаза и т.п.). Отличительная особенность биометрических технологий заключается в относительной простоте и удобстве для пользователей, проходящих процесс идентификации для совершения трансакции или прохода в офисное здание. В то же время, с началом пандемии, необходимостью носить маску и перчатки, сфера

использования популярных факторов биометрии заметно сократилась.

Выход из положения Марулис видит в активном внедрении «поведенческой биометрии». Она основывается на уникальных особенностях и привычках любой личности, проявляемых в манере ходить, двигаться, работать на клавиатуре компьютера или смартфона, говорить. Это динамические методы, оценивающие уникальные свойства поведения пользователей, которые, как считают специалисты, «в будущем смогут значительно сократить риски в сфере безопасности и сделают более надежной защиту данных, устройств и объектов по сравнению со статическими биометрическими методами» (rb.ru/story/behavioural-biometrics/).

Поведенческую биометрию некоторые специалисты называют пассивной, потому что пользователям не нужно совершать никаких дополнительных действий при выполнении операции. «Им не нужно прикладывать палец к специальной кнопке или говорить в микрофон. Они ведут себя как обычно. К тому же поведенческая биометрия позволяет выявлять мошенничество на ранних этапах, еще до самого действия злоумышленников. Это должно помочь компаниям и пользователям уменьшить убытки, а также удешевить биометрические системы. Меньший объем инвестиций в подобные решения (в сравнении с используемыми сегодня) связан и с тем, что поведенческая биометрия работает на всех смартфонах благодаря сенсорам, которые уже установлены на этих устройствах» (secuteck.ru). .

Леандро Маргулис называет области активного применения поведенческой биометрии:

1. *Физический доступ* в дом, офис или автомобиль со смартфоном в кармане или сумке, приложение которого автоматически открывает дверь. Продвинутые модели с технологией машинного обучения позволяют подтверждать, что мобильный телефон именно в ваших, а не чужих руках, и что именно вы, а никто другой, идет по направлению к данной двери.
2. *Трансакции* – как онлайновые, так и непосредственно в офисе или магазине.
3. *Распознавание и отличие человека от робота.*

# Три фундаментальных принципа в работе Центра оперативной безопасности

Современный бизнес, как никогда ранее, нуждается в усилении корпоративных программ безопасности, пишет Патрик Броснан в издании Security Magazine, August, 2021. Ландшафт угроз и рисков настоятельно требует как эффективного прогнозирования, так и ситуационного анализа в реальном времени, чтобы успешно минимизировать риски для бренда, персонала, имущества, клиентов. Многие крупные компании обращаются к идее создания Центра оперативной безопасности (SOC - Security Operations Center). Такой Центр охватывает широкий спектр функций, в том числе видеонаблюдение, СКУД, тактическую и стратегическую разведку, кибербезопасность.

Броснан выделяет три главных, по его мнению, фактора успешной работы Центра оперативной безопасности.

1. Тесная координация внутренних и внешних разведывательных ресурсов компании

К внутренним, т.е. собственным ресурсам автор публикации относит системы СКУД, камеры видеонаблюдения, службу безопасности, кадровую службу. Чем лучше обеспечен (технологиями и специалистами) мониторинг и анализ, тем более правдивую картину угроз и рисков вы получаете.

Среди внешних ресурсов разведки Броснан называет правоохранительные органы власти, социальные сети, новостные источники, официальные правительственные сообщения и заявления, прочие информационные ресурсы в свободном доступе, а также dark web – теневой сегмент Всемирной паутины.

2. Стандартизация

Независимо от того, расположен ли ваш Центр оперативной безопасности в одном месте или разбросан по разным регионам, решение поставленных перед ним задач во многом определяется уровнем стандартизации технологий безопасности. Все компоненты корпоративной технологической инфраструктуры должны быть совместимыми между собой, интегрированными на единой платформе. В противном случае, когда информационные ресурсы работают независимо друг от друга, технологически не совпадают, не взаимодействуют, велик риск «проморгать» угрозу. Броснан рекомендует при приобретении новых технологий и оборудования обращать особое внимание на этот аспект.

3. Централизация

Ценность региональных отделений состоит в том, что они максимально приближены и учитывают географические, этно-культурные, социально-экономические особенности местности в большой стране. В еще большей мере это относится к зарубежным филиалам корпорации. Замечено, что региональные офисы подвержены, как правило, центробежным тенденциям. Это чревато функциональными нарушениями в деятельности организации. Наиболее эффективная модель, способная преодолеть данное нежелательное явление, предполагает высокую степень централизации и стандартизации. Все технологические и операционные процессы жестко контролируются головным офисом. Поступающие данные мониторинга синтезируются, обрабатываются и анализируются в единой системе. Только так разведка может быть результативной.

Без такого Центра оперативной безопасности, пишет автор статьи в заключение, крупная компания может оказаться в информационном «вакууме». Для создания Центра требуются немалые усилия. Прежде всего, рекомендует он, продумайте, что лучше – иметь полностью собственный Центр или воспользоваться услугами аутсорсинга для некоторых функций. Последний вариант наиболее предпочтителен, когда не хватает финансовых и кадровых ресурсов для решения всех задач корпоративной безопасности собственными силами. Каким бы путем вы ни пошли, инвестиции в этой сфере имеют стратегическое значение для будущего вашего бизнеса.

# Как киберкриминал превращает похищенные данные в доллары

В первом полугодии 2021 года, по данным экспертов, многие гиганты цифровой экономики стали жертвами утечек информации, как непреднамеренных, случайных, так и обусловленных атаками хакеров, действиями инсайдеров. Среди них - Facebook, LinkedIn, Instagram.

Злоумышленники очень изобретательны в добывании информации, говорит Джон Кинселла из компании Accurics (решения по информационной безопасности). Они действуют по формуле «курица по зернышку клюет»: там и сям собирают по крупице данные, которые накапливают в своей базе. В одном случае выясняют имя и фамилию интересующей их личности. Во втором –электронный адрес. В третьем - интересы и предпочтения намеченной жертвы. «Сами по себе такие данные не выглядят важными, но, будучи соединенными в одном месте, могут представлять интерес с точки зрения организации фишинговой атаки» (Chief Security Manager, June 1, 2021).

Сбор и агрегация данных – только первый шаг, замечает Кинселла. В условиях растущей специализации и разделения труда в мире киберкриминала сборщик данных может сдать информацию «в аренду» непосредственным организаторам фишинговых кампаний за определенную сумму. Но может и самостоятельно провести взлом сети с последующим торгом. В зависимости от квалификации и намерений.

Собираемые воедино крупинки информации являют собой реальную угрозу компаниям и персоналиям. Адреса электронной почты, например, могут быть использованы для конкретизации, детализации внутренней иерархической структуры компании, для анализа коммуникаций между работниками. Все это необходимо для успешной реализации тактики социальной инженерии. У хакеров нет необходимости атаковать большое число лиц в одной компании. Достаточно выбрать одного-двух из числа тех, кто беспечно выгружает в свой компьютер зараженное вирусом приложение, «кликает» на непроверенную ссылку, отправляет учетные данные непонятно куда и зачем.

Один из популярных у хакеров приемов – войти в доверие к намеченной жертве, используя интернет чаты, электронную переписку. Преступники ловко играют на привычке множества любителей откровенничать в интернете о себе, своей семье и работе.

Они эксплуатируют доверчивость для успешного претекстинга (pretexting – выдача себя за другого человека с целью получения информации, недоступной иными, легальными путями). Например, хакер узнает, что конкретная фирма пользуется услугами платежной компании (payroll company). Он/она звонит на фирму конкретному работнику будто бы от имени платежной компании и доверительно сообщает, что в связи с обновлением интернет системы услуги будут скорректированы, о чем вскоре последует официальное уведомление и соответствующие инструкции. Он может вновь, и не раз, повторить звонок, не требуя никаких действий, укрепляя доверительный контакт. Затем выходит на связь уже с реальными инструкциями, которым, как нередко случается, жертва вслепую следует, не проверяя и не перепроверяя информацию. В результате, говорит Роджер Граймс (компания KnowBe4,

провайдер тренингов по ознакомлению персонала с интернет рисками и угрозами), организация может лишиться десятков и сотен тысяч долларов, «что и происходит почти ежедневно» (там же).

Общепринято считать, что если хакер не владеет критически важной информацией, например, данными кредитной карты, то все другое, что он о вас знает, не имеет принципиального значения. По мнению Тревора Моргана, старшего менеджера Comforte AG (защита и безопасность кредитных карт и других финансовых инструментов), это большая ошибка. Хакер начинает сбор персональной информации с самых простых, невинных, на первый взгляд, данных. Например, о вашем домашнем адресе, электронной почте, имени пользователя (username).

Это только первый шаг в операции хищения идентификационной информации. «Главный риск заключается в том, что, собрав достаточно много персональных данных, хакер может открыть новые аккаунты от вашего имени», подчеркивает Морган. «А если хакер с этого ничего для себя не «намоет», то может просто продать похищенную информацию другим злоумышленникам для фишинговой атаки, либо сомнительным маркетинговым организациям, которые обрушат на вас лавину непрошенной рекламы» (там же).

Аналогичному риску подвергается и организация, где вы работаете. Вы запросто можете стать объектом фишинговой атаки, нацеленной на кражу интеллектуальной собственности или на иной ущерб.

# Главные риски и угрозы для национальных систем здравоохранения в 2021 году

Киберкриминал в полной мере воспользовался новыми возможностями, открытыми пандемией коронавируса, в частности, вынужденным расширением дистанционных медицинских услуг, для наращивания атак на системы здравоохранения по всему миру. Хакеры охотятся за ценными данными пациентов и компаний. В этом им помогает технологическая отсталость средств информационной безопасности во многих поликлиник и больниц, не имеющих средств на инновации.

Журнал Chief Security Officer (17 June, 2021), опираясь на мнения ряда экспертов, формулирует основные угрозы для здравоохранения.

*Вымогательские атаки*

Преступники давно осознали, что медицинские учреждения, отвечающие за здоровье и жизни пациентов по сравнению с другими отраслями экономики и бизнеса более сговорчивы в торге за выкуп похищенных и зашифрованных данных. Компания Tenable (разработчик программных решений для мониторинга информационной безопасности корпоративных сетей) изучила около 300 публично заявленных взломов сетей американских медучреждений за период с января 2020 по февраль 2021 года. В более чем половине случаев речь шла о шантаже и вымогательстве.

Как полагают эксперты, наибольший риск связан с электронным хранением историй болезни и других медицинских записей. К. Барлоу, глава компании CynergisTek (услуги в области кибербезопасности) отмечает, что успешная атака вымогателей чревата закрытием доступа к критически важной информации, например, к рецептам многокомпонентных лекарств для тяжелобольных диабетом или раком. Что еще хуже, хакеры могут сознательно исказить рецептуру.

Проблема усугубляется и тем, что сегодня страховые компании отказываются компенсировать выплаты шантажистам по причине плохой защиты данных (отсутствие двухфакторной аутентификации, технологий реагирования и прочее).

*Уязвимости облачных решений*

В последние годы все больше медицинских организаций пользуются облачными услугами в процессе перехода к цифровым технологиям. Такая тенденция объективно расширяет пространство для хакерских атак. Причем одно медучреждение нередко обслуживается разными облачными организациями, каждая из которых имеет собственный стандарт безопасности, что, конечно, мешает проводить единую, цельную политику информационной защиты.

Опрос, проведенный среди организаций здравоохранения компанией Infoblox (разработчик средств автоматизации сетевого администрирования), дал такие результаты:

- 53% респондентов заявили о взломах облачных решений за последние 12 месяцев;

- 34% организаций, подвергшихся вымогательским атакам, потеряли два и более миллионов долларов каждая.

*Атаки на веб-приложения*

Компания Imperva (программные решения и услуги кибербезопасности) провела свое исследование, показавшее 50%-й рост атак на веб-приложения медучреждений в 2020 году. Компания утверждает, что ежемесячно фиксировала около 200 миллионов хакерских атак на систему здравоохранения США. Цифра фантастическая! Особенно уязвимыми оказались данные в госпиталях, передаваемые из внутренних сетей на внешние удаленные объекты.

*Трафик плохих ботов (программ – роботов)*

Еще одна проблема – плохие боты, т.е. роботы, предназначенные для хищения информации с веб-сайтов, распространения спама, загрузки нежелательного софта и прочих нехороших дел. Упомянутая выше компания Imperva выявила 372%-е увеличение числа атак этих роботов на веб-сайты в системе здравоохранения с сентября 2020 по май 2021 гг. Боты могут не только красть учетные данные, логины и пароли, но и изменять содержание сайтов.

*Фишинг*

Это, пожалуй, самая опасная после вымогательских атак угроза для здравоохранения. Исследователи зафиксировали 189%-й рост фишинговых атак на аптеки и госпитали США между декабрем 2020 года и февралем 2021 года. За тот же период времени атаки, связанные с кампанией вакцинации, выросли на 530%.

Healthcare Information and Management Systems Society (некоммерческая организация, преследующая цели улучшение системы здравоохранения в США посредством информационных технологий и инновационных систем управления) в ходе опроса профессионалов кибербезопасности в отрасли здравоохранения пришла к таким результатам:

- 57% респондентов признали, что их организации подверглись фишинговым атакам;

- 20% отметили использование криминалом приемов социальной инженерии;

- именно фишинг используется чаще всего для компрометации корпоративных данных.

# Инсайдерские угрозы и экстремистская риторика

Частота инцидентов безопасности, связанных с преднамеренными инсайдерскими угрозами, с 2018 по 2020 гг. увеличилась почти на 50%. Об этом говорится в аналитическом исследовании Ponemon Institute «Цена инсайдерских угроз в 2020 году». В нем отмечается не случайное совпадение роста инсайдерства и политической экстремисткой риторики, как слева, так и справа, особенно в социальных сетях.

Авторы исследования, в частности, отмечают: «Бизнес и профессионалы корпоративной безопасности единодушны во мнении, что стремительный рост инцидентов, связанных с инсайдерами, во многом обусловлен переводом персонала компаний на домашнюю работу в прошлом году. Две трети опрошенных руководителей информационной защиты заявили, что их организации подверглись злонамеренным инсайдерским утечкам весьма чувствительной служебной информации. Более половины респондентов считают неизбежным рост инсайдерских рисков в обозримом будущем. Риски проистекают из-за слабого контроля по доступу работников к корпоративным данным, в том числе, и тех, кто по своим функциям не должен иметь допуск, но им пользуется. Несмотря на такую мрачную тенденцию, половина организаций не озабочена подготовкой плана противодействия инсайдерским угрозам» (Security Management, June, 2021).

Журнал Security Management перечисляет индикаторы потенциальных инсайдерских рисков:

- атрибуты доступа в корпоративную сеть (кто и какие разрешения имеет);

- соотношение между результатами работы и карьерного роста;

- зарубежные связи;

- нарушения правил и инструкций по безопасности;

- поведение, характеризуемое фактами насилия, агрессии, злоупотреблений;

- финансовые аспекты (например, наличие задолженности);

- аномальное поведение, плохие отношения с коллегами;

- особенности характера, психики.

Чтобы обнаружить и оценить потенциальную инсайдерскую угрозу, исходящую от конкретного лица, требуется ответить на ряд вопросов:

- Происходит ли у подозреваемого работника ухудшение производственных показателей?

- Поступали на него/нее жалобы, например, в отдел кадров?

- Имеет ли выговоры по работе?

- Обладает ли большими, чем необходимо для работы, привилегиями по допуску к служебным секретам?

- Как часто ездит за границу?

- С кем ведет переписку и поддерживает иные связи с иностранцами?

- Нарушал ли инструкции по безопасности?

- Стремится ли работать во внеурочные часы в офисе?

- Живет ли по легально заработанным средствам?

- Имеются ли налицо факты насильственного поведения, незаконного владения оружием, употребления наркотиков, попыток фальсификации корпоративных данных, а также экстремистских заявлений?

Один лишь из перечисленных признаков говорит немногое. Но в сочетании с другими требует более пристального внимания.

В своих программных документах организация The National Insider Threat Task Force (NITTF), созданная в недрах американских государственных служб безопасности после скандала WikiLeaks, отмечает:

«Критически важно удостовериться, что подозреваемая личность в своих действиях не преследует криминальных целей, но просто нуждается в поддержке и помощи. ….Необходимо оказать помощь тем, кто ощущает себя в сложной ситуации, и выход из нее видит в совершении отчаянного акта, будь то насилие на рабочем месте, саботаж, суицид, или шпионаж. Своевременное вмешательство может сохранить сотруднику работу и карьеру, спасти жизни, защитить важную информацию» (там же).

# Внешние угрозы и разведка из открытых источников

Инфраструктура физической охраны традиционно включает известный набор

инструментов и средств: камеры, СКУД, периметр безопасности, система обнаружения вторжений и т.п. Но одно дело – охрана территории объекта, другое – контроль того, что происходит за пределами периметра, на прилегающих территориях, откуда могут приходить реальные угрозы. Такие, например, как массовые протесты и беспорядки.

Марк Эшворд, автор статьи в журнале Security Management, обращает внимание на такой инструмент защиты от внешних угроз как разведка из открытых источников (open-source intelligence), т.е. сбор информации из открытых, общедоступных источников, как онлайновых, так и оффлайновых. Информация сама по себе, подчеркивает автор, еще далеко не разведка. Ее необходимо систематизировать, анализировать, трансформировать в конкретные выводы и заключения, необходимые для своевременной и точной оценки рисков.

Разовая разведывательная операция с течением времени, по мере изменений в ландшафте угроз, теряет свою актуальность . Поэтому, подчеркивает Эшворд, данному процессу необходимо придать постоянный или, по крайней мере, регулярный, систематический характер, не забывая о полном цикле разведки: планирование, разработка стратегии поиска, процессинг данных, структурированный анализ, отчет о результатах для тех, кто принимает решения.

Критически важен выбор зоны, территории, где носители потенциальных угроз наиболее активны. В интернете объектом пристального внимания могут быть чаты и форумы, где намерения таких игроков раскрываются наилучшим образом. К примеру, лица и группы людей с экстремистскими наклонностями, действующие в непосредственной близости от охраняемого объекта, обычно предпочитают открытое обращение к общественности, подталкивая ее к тем или иным шагам. Фиксация их порталов, участия в чатах – необходимая предпосылка успешной разведки.

Без планирования, правильно составленной инструкции (руководства) бессистемный, не структурированный мониторинг колоссальных массивов данных малоэффективен. Разведзадание должно быть практичным и реалистичным. Автор предостерегает от попыток прогнозировать непредсказуемое. В то же время он использует термин «вероятностный анализ», подразумевающий идентификацию наиболее реального исхода (из множества вариантов) того или иного предполагаемого события или тенденции. Практически речь идет об определении, о выборе источников информации относительно прогнозируемого события, предназначенных максимально снизить уровень неопределенностей.

Планирование разведоперации предполагает избавление от предубеждений, предвзятостей, пристрастности и прочих личностных характеристик, которые, так или иначе, воздействуют на процессы анализа, могут привести к ошибочным выводам и заключениям. Автор, в частности, указывает на такой широко распространенный недостаток как сверх полагание, некритический упор на снятый первый, внешний слой информационного массива, который попадает в руки и нередко служит материалом для поспешных умозаключений.

Тщательное планирование также поможет определить наиболее важные, первостепенные для разведки информационные ресурсы, что важно для экономии средств и времени, снижения воздействия необъективных факторов на сбор и анализ информации. Кроме того, отмечает Эшворд, «вероятностный анализ» на стадии планирования информационной разведки способствует решению проблемы точности, адекватности информации, когда имеешь дело с такими ненадежными источниками

как социальные сети, несущие массу дезинформации, искаженных представлений и злонамеренной лжи.

*(продолжение в следующем выпуске нашего журнала)*

# Платить или нет хакерам-вымогателям?

Американский Institute for Security and Technology опубликовал рекомендации относительно защиты от хакерских атак, преследующих цель шантажа и вымогательства. В выработке рекомендаций участвовали десятки экспертов, работающих в охранных предприятиях, госучреждениях, силовых структурах, международных организациях, гражданских обществах.

Во время обсуждений, пишет издание Chief Security Officer, July 5, 2021, одним из центральных вопросов была дилемма: идти на уступки вымогателям или нет, платить или отказывать.

Высказывались разные точки зрения, включая такие радикальные как «категорический запрет на платежи», «всеобщий отказ от криптовалюты». Джен Эллис, директор по общественным связям компании Rapid7 (производитель продуктов для безопасности сети, совместимости политик безопасности и тестирования систем защиты IT-инфраструктуры) полагает, что такой подход принесет скорее вред, чем пользу: «Запрет на выплаты заставит хакеров выбирать своей целью наиболее слабые, уязвимые с точки зрения финансовой устойчивости и уровня кибербезопасности организации. Последние, чтобы спасти бизнес, будут вынуждены идти на тайный сговор с преступниками, выплачивать деньги, несмотря на запреты. Тем самым они станут еще более зависимыми от криминала».

Что же касается криптовалюты, то от ее запрета пострадают и те, кто легально ею пользуется, добавляет Эллис. Вместо ограничений эксперты рекомендуют усилить контроль за трафиком криптовалюты. Это легче всего делать при попытках криминала конвертировать биткойн в обычную валюту – процесс, в котором не обойтись без банковской системы.

Вопрос - платить или не платить вымогателям – чрезвычайно сложный, говорит Радж Самани, главный аналитик McAfee (антивирусное ПО). Чтобы ответить на этот вопрос, необходимо принять во внимание массу вещей и аспектов. Ведь многие организации и компании попросту не имеют иного выбора, кроме как платить, поскольку не обладают компетенциями и ресурсами для восстановления работы в минимально необходимые сроки и без большого ущерба для бизнеса. Это, например, касается лечебных учреждений, где блокировка данных угрожает здоровью и жизням пациентов.

Все это понимает и использует киберкриминал. Согласно опросу, проведенному Chainalysis (предоставление данных, программного обеспечения, услуг и исследований по кибербезопасности), в 2020 году сумма выплат вымогателям по сравнению с предшествующим годом возросла на 341% и достигла почти полумиллиарда долларов США.

Institute for Security and Technology рекомендует организациям не скрывать факты инцидентов безопасности. В каждом случае ставить в известность компетентные органы. Решению «платить или нет» должен предшествовать серьезный анализ, что собой представляет хакер или группа хакеров, замечен ли он/она/они в подобных атаках на другие организации, как себя вели в переговорах и т.д. Такой анализ проделать самостоятельно, без внешней поддержки госорганов практически невозможно.

Если компания решает платить, то, по крайней мере, надо попытаться сбить запрашиваемый выкуп, отмечает Марк Гренс, президент компании DigitalMint (консультирует и помогает жертвам вымогательства в переговорах с хакерами). По опыту известно, что вымогатели обычно склонны к компромиссу. Но иногда выплата не решает проблему. Многие компании, заплатившие шантажистам, подверглись повторной атаке.

Наиболее эффективный путь, уверены эксперты, это вкладывать средства в технологии кибербезопасности, способные защитить бизнес. Также эксперты подчеркивают необходимость широкого международного сотрудничества в борьбе с киберкриминалом. И в этой связи позитивно расценивают соответствующие договоренности, достигнутые на переговорах в Женеве между президентами России и Америки.

# Охрана предприятия: статья расходов или доходов?

Бурке Броунфелд пишет в журнале Security Magazine (June, 2021) о сложившемся среди многих бизнесменов ошибочном стереотипе относительно корпоративной безопасности как о важной, но абсолютно затратной функции компании. Автор публикации считает необходимым бороться с этим заблуждением, формировать образ охраны как ресурс добавленной стоимости, а не источник сплошных убытков.

*Преодолевайте изоляционизм службы безопасности*

Часто проект безопасности в компании плохо увязывается, либо вообще не упоминается в связи с задачами бизнеса. Эту традицию необходимо ломать. Наилучший способ – разобраться, в чем состоят цели и стратегии компании через содержательные беседы и обсуждения с акционерами и ключевыми топ-менеджерами. Не стесняйтесь спрашивать «зачем» и «почему», чтобы уяснить, какую роль играет безопасность в реализации задач, стоящих перед компанией.

Автор приводит выдуманный им эпизод. Допустим, вы начальник СБ в корпорации Starbucks, обладающей десятками тысяч ресторанов по всему миру, рекламирующей и продвигающей «самый лучший в мире кофе». Кофе добывается в странах третьего мира с неустойчивой, нередко взрывоопасной политической ситуацией. Обеспечение безопасности всей цепочки поставок, начиная с кофейных плантаций – одна главных задач корпоративной безопасности, от решения которой напрямую зависит доходность бизнеса. Рассуждая таким путем, вы непременно приходите к итоговой строке («bottom line») в бюджете компании.

*Не злоупотребляйте ответами «да» или «нет».*

Многие занятые в охранной индустрии профессионалы вышли из силовых структур. Они привыкли односложно реагировать на многие вещи, сообразуясь с правилами, что можно, а что нет. Между тем, бывают ситуации, на которые односложно реагировать нельзя. Автор предлагает еще один пример. Вы, положим, директор СБ компании по производству одежды. Акционеры решили перевести часть производства в страны с дешевой рабочей силой, скажем в Пакистан, на границах которого всегда неспокойно. С точки зрения безопасности такой шаг весьма рискован. Но генерального директора компании вы не удовлетворите краткой реакцией «нет» или «да» новому проекту. Ваша задача в данной ситуации собрать максимум информации о предполагаемых рисках, о том, какие меры могут их предупредить или, по крайней мере, минимизировать, наконец, во сколько обойдутся компании дополнительные мероприятия по обеспечению безопасности нового бизнеса. Развернутый, детальный анализ поможет прийти к заключению, что риски терпимы либо слишком высоки.

*Помните, что охрана – неотъемлемая часть бизнеса предприятия*

Корпоративную безопасность нельзя рассматривать в отрыве от продаж товаров и услуг, которыми занимается компания. Охрана «продает» имидж и бренд компании, начиная с рядового охранника на пропускном пункте, который первым встречает клиента или партнера. В наше неспокойное, турбулентное время вопрос безопасности для людей вышел на первый план. Он встал в один ряд с критериями качества товара/услуги и его цены. Сегодня намного очевиднее просматривается связь между охраной и продуктом, чем еще 20-30 лет назад.

*Как вы выглядите, так выглядит и компания*

Бурке Броунфелд подчеркивает значение внешнего вида, поведения и манеры общаться начальника и сотрудников СБ для имиджа и бренда компании. Он, в частности, рекомендует обращать особое внимание на участие в общественных мероприятиях – конференциях, выставках, деловых совещаниях, предполагающих встречу с новой аудиторией, которая подсознательно связывает руководителя или представителя СБ, со вкусом одетого, хорошо информированного, мыслящего перспективно, неплохого оратора с брендом компании, в которой он работает.

# Уроки пандемии для корпоративной безопасности

Журнал Security Management (June, 2021) опубликовал интервью с Дэвидом Фини, директором по управлению рисками консалтинговой корпорации Deloitte Risk and Financial Advisory, в котором он ответил на вопросы, связанные с возвращением людей в офисы и цеха после вынужденной самоизоляции и т.н. «удаленки».

*Как повлиял COVID-19 на роль и место профессионалов корпоративной безопасности в бизнесе?*

Любой серьезный кризис подчеркивает важность, приоритетность функции

безопасности в организации. Это мы наблюдаем с началом пандемии коронавируса. Первое, что бросается в глаза, - растущее участие акционеров, владельцев бизнеса в разработке кризисных планов. С другой стороны, профессионалы корпоративной безопасности стали намного чаще приглашаться на совещания с первыми лицами и топ-менеджментом. Причем не только по вопросам охраны, но и по проблематике стратегического бизнес планирования. Организации сегодня отдают себе отчет, что возвращение сотрудников на рабочие места в офисах и на производстве не может происходить успешно без учета факторов безопасности.

Даже те бизнесмены, кто ранее скептически смотрели на функцию безопасности, пренебрегали кризисным планированием, теперь, по мнению Фини, гораздо внимательнее и серьезнее относятся к управлению рисками и разработке соответствующей стратегии на случай новых кризисов. Для профессионалов корпоративной безопасности это хороший шанс улучшить взаимодействие с бизнесменами, понимая и разделяя их приоритеты, цели, озабоченности и ценности.

*Какова роль корпоративной безопасности в процессе возвращения людей на свои рабочие места после длительного периода работы дома?*

Во многих компаниях службы безопасности полностью вовлечены в этот процесс. Например, организуют с персоналом специальные тренинги по ознакомлению с рисками и угрозами, используя новый опыт, приобретенный во время пандемии.

*Что стало с кризисными планами, составленными еще до пандемии? Пришлось ли их коренным образом переделывать? Как в этой работе участвуют сами бизнесмены?*

Надо периодически пересматривать форс-мажорные планы, тем более, после кризиса. Но не отбрасывать их прочь, даже в том случае, когда те или инциденты случились из-за ошибок планирования. Любой серьезный кризис требует корректировки кризисного планирования, включая методологию. Вовлеченность владельцев бизнеса в процесс такого планирования всегда возрастает после кризиса. И этим надо пользоваться для укрепления отношений между СБ и бизнесменами.

*Какие новые, либо ранее недооцененные проблемы требуют к себе акцентированного внимания с учетом уроков пандемии COVID-19?*

Приоритетного внимания требует к себе обеспечение безопасности цепочек поставок, которые наиболее сильно пострадали в период пандемии. Мы своими глазами увидели долгосрочные разрушительные последствия из-за сбоев в таких цепочках. Это понимают и бизнесмены, и профессионалы корпоративной безопасности.

*Какова роль специалиста по управлению рисками в процессе возобновления бизнеса,*

На вопрос владельца компании, обращенный к профессионалу корпоративной безопасности, открывать офис или еще рано, могут последовать встречные вопросы. Например, каковы условия, необходимые для возобновления нормальной работы компании, какие цели ставит бизнесмен, желая вновь открыть офис или производство, какие риски для него абсолютно не приемлемы. Начальник СБ может предложить конкретную стратегию минимизации потенциальных рисков, которыми чревато возобновление работы организации.

Фини обращает внимание, что в отношениях между правлением и СБ характерный

прежде административно-директивный стиль постепенно уступает месту другому формату, когда директор или менеджер корпоративной безопасности выступает не в качестве дисциплинированного подчиненного, но в роли советника, которому доверяют, и чье мнение учитывают при принятии стратегических решений.

# Охрана спортивных объектов во время пандемии

Для многих американских любителей бейсбола этот спорт стал неотъемлемой частью образа жизни. На стадион они приходят не только «поболеть» за любимую команду, но и пообщаться с друзьями, завести новые знакомства, т.е. игры - важное место социальной «тусовки». В 2020 году из-за пандемии коронавируса трибуны опустели. «Игра команд без зрителей выглядит сюрреалистично», - замечает Д. Мелкер, директор безопасности команды «Сент-Луис Кардиналс» (штат Миссури), выступающей на домашнем стадионе Busch Stadium.

Этот стадион расположен в самом центре Сент-Луиса, по соседству с офисами крупнейших компаний и госучреждений. «Поэтому мой взгляд на охрану не замыкается территорией стадиона, он распространяется на соседние объекты», - говорит Мелкер (Security Management, July, 2021). Для него чрезвычайно важно тесное сотрудничество с коллегами по корпоративной безопасности из близлежащих компаний и организаций. Каждый раз, проводя оценку рисков для стадиона, он приглашает соседей совместно поучаствовать в анализе ситуации. «Это одинаково полезно и для нас, и для них», - говорит он.

В связи с сокращением втрое числа игр и карантинными мерами в 2020 году 90% работников стадиона были отправлены на «удаленку». В наименьшей степени это коснулось охранников, которые продолжали нести службу при закрытых дверях, в условиях резкого роста политической нестабильности (протесты, включая движение Black Lives Matters) и городской преступности. В окрестностях стадиона появилось много бездомных. Охране пришлось вступить с ними в прямой контакт. Конечно, замечает Мелкер, можно было бы попросить полицию «очистить» территорию вокруг спорткомплекса, но «мы предпочли более гуманный, человеческий способ предупредить инциденты безопасности».

Во время игр зрители отсутствовали, но для них выставлялись огромные трансляционные экраны на соседних улицах, автомобильное движение по которым на эти часы по просьбе клуба перекрывалось.

Родным домом для другого бейсбольного клуба - Blue Jays - всегда был и остается Rogers Centre в канадском городе Торонто. Но поскольку правительство из-за пандемии закрыло границы, команде пришлось в 2020 году временно перебраться сначала в Буффало, город в северно-западной части штата Нью-Йорк, а в 2021 году во Флориду.

В интервью журналу Security Management вице-президент клуба, отвечающий за безопасность, Марио Коутиньо полагает, что пандемия наряду со всеми очевидными минусами способствует развитию передовых технологий и их адаптации к протоколам

безопасности. Пример – быстрый переход от бумажных билетов к цифровым, позволяющий лучше прослеживать тенденции среди болельщиков, что важно для службы безопасности клуба. Коутиньо добавляет, что новые инструменты анализа данных будут использованы после возвращения на родной стадион для того, например, чтобы избавиться от толкотни на входе перед началом игры. Клуб Rogers Centre располагается в центре Торонто и не имеет собственного паркинга, поэтому болельщики добираются обычно общественным транспортом. Длинные очереди и заторы возникают в точках пропуска с металлическими рамками, где проверяются билеты и сумки.

С началом сезона 2021 года в MBL, главной лиге бейсбола, спортивная жизнь постепенно возвращается в нормальное русло. Клуб Philadelphia Phillies разрешил части зрителей приходить и болеть на принадлежащем команде стадионе Citizens Bank Park. Естественно, при соблюдении санитарной дистанции и ношении масок. Директор безопасности клуба Сал ДеАнжелис ужесточил меры контроля. Зрителям запрещено проносить с собой сумки и рюкзаки. Запретом не охватываются медицинские, гигиенические пакеты и небольшие сумки размером не превышающие 16x16x8.

До эпидемии на некоторых стадионах болельщикам разрешалось контактировать с игроками в специально выделенной для этой цели зоне. Сейчас везде эти зоны закрыты. Журналистам тоже существенно ограничены прямые, личные контакты с игроками и тренерами. «Этой традиционной практике положен конец. И я не знаю, когда она вернется в спорт», - сетует Мелкер.

# Кибербезопасность: успешная история Токийской Олимпиады

Задолго до Олимпийских игр в Токио разведки и эксперты многих стран предупреждали о потенциальной опасности кибератак и призывали к предупреждению инцидентов, подобных тем. что случались на предыдущих Играх в Бразилии, Южной Корее, Великобритании. «К счастью, - пишет журнал Security Magazine, - Международный олимпийский комитет и Организационный комитет страны-хозяйки не нужно было убеждать. В ходе Игр стало очевидным, что организаторы приняли все возможные и необходимые меры, и, несмотря на вызовы, обусловленные эпидемией коронавируса, токийская Олимпиада явила успешную историю с точки зрения кибербезопасности».

Эксперты полагают, что опыт этой олимпиады может быть весьма полезен организаторам планируемых крупных спортивных состязаний.

Один из главных принципов, которым следовали организаторы Олимпиады в Токио, заключается в формуле «лучшая защита – это атака». Принцип, хорошо известный спортсменам. В сфере кибербезопасности распространена практика пассивного ожидания до тех пор, пока «петух не клюнет». Такое отношение – прямой путь к катастрофе. Степень киберугроз сегодня стремительно увеличивается. Только вымогательские программы за последний год приросли на 50%. Популярные

спортивные игры, как, например, международные чемпионаты по футболу, организация и проведение которых во все большей мере строится на основе цифровых технологий, пользуются повышенным вниманием киберкриминала. Все это было известно и учтено организаторами Токийской Олимпиады.

Хотя не обошлось без мелких инцидентов, например, утечки персональных данных ограниченного числа обладателей билетов на игры, серьезных сбоев, таких, что случились в Пхёнчхане, где кибератаки едва не сорвали церемонию открытия зимних Олимпийских Игр, удалось избежать.

Эксперт и журналист Брайан Гант, анализируя работу и результаты киберзащиты на Токийской Олимпиаде, обращает внимание на важную роль аналитиков поведенческих характеристик в предупреждении инцидентов безопасности. Они успешно справились с задачами интерпретации данных в цифровом трафике, систематизации и обработки тревожных сигналов, планировании упреждающих контратак. (Security Magazine, August, 2021). Их успех был бы невозможен без высококлассных специалистов мониторинга, которые денно и нощно, по 24 часа в сутки, отслеживали трафик в режиме реального времени, собирали все подозрительные сигналы, очищали их от информационного мусора, передавали экспертам по анализу поведенческих отклонений.

Поскольку Олимпийские Игры в наше время практически неотделимы от политики и дипломатии, в этом деле принимали участие спецслужбы ряда стран, в их числе ФБР (США) и МИ5 (Великобритания). По мнению Брайана Ганта, вся работа по безопасности, включая кибербезопасность, координировалась из «объединенного командного центра» (a joint command center). Одновременно привлекались и частные охранные предприятия, в частности, японские, тайваньские, израильские (Security Magazine, August 17, 2021).

Решающее значение, полагает автор публикации, имело активное, превентивное, жесткое противодействие известным группировкам и игрокам в мире киберкриминала, деятельность и поведение которых начали плотно отслеживать задолго до Игр. Гант не раскрывает детали превентивных мер, принятых относительно тех, от кого исходила наибольшая потенциальная угроза, но сам факт, что преступникам не удалось вторгнуться и помешать нормальному проведению Олимпиады, свидетельствует о «несомненном успехе» упреждающих шагов и действий.

Тактика хакеров постоянно меняется и совершенствуется, не позволяя почить на лаврах, самоуспокаиваться, расслабляться, подчеркивает Гант. Но принимая во внимание, что на фоне угрожающего роста киберпреступности в мире организаторам Токийской Олимпиады удалось нейтрализовать потенциальные угрозы, можно с определенным оптимизмом смотреть в будущее, учась не только на провалах и ошибках, но и на успешном примере прошедших в столице Японии Игр.

# Пандемия и организованная преступность в Европе

Весной 2021 года испанская полиция арестовала членов международной преступной

группировки, конфисковав более полтонны гашиша, готового к отправке во Францию и Италию. Это событие привлекло к себе особое внимание, поскольку полицейские обнаружили у преступников недостроенную самодельную подводную лодку. Длиной 9 метров она могла перевозить до двух тонн наркотиков.

Сам по себе факт довольно необычный. По мнению журнала Security Management, он наглядно иллюстрирует наглость преступного мира, возросшую с началом пандемии коронавируса и последовавшей за ней «экономической турбулентностью с элементами глобального хаоса».

В опубликованном в апреле с.г. докладе Европола «Serious and Organised Threat Assessment» говорится, что 40% криминальных группировок в странах Евросоюза вовлечено в нелегальную торговлю наркотиками. Каждая вторая использует насилие как часть преступного бизнеса. А 80% прикрываются легальным бизнесом.

Отчет Европола констатирует, что преступный мир действует в 2021 году более гибко и изощренно. Мелкие группки координируют свою деятельность с помощью нелегальных или псевдо-легальных консультантов, оказывающих им помощь в сфере законодательства, финансов, логистики, и в других вещах.

Терроризм и организованная преступность остаются главными внутренними угрозами в Евросоюзе, отмечается в докладе. «Торговля кокаином, каннабисом, синтетическими наркотиками и психотропными веществами представляют ключевую угрозу для Евросоюза, если принять во внимание уровень насилия, которым сопровождается наркоторговля».

Каждая четвертая банда, связанная с наркотиками, действует более 10 лет. 40% обладают иерархической структурой управления. 79% имеют в своем составе 6 или более членов. 180 национальностей занимаются этим преступным промыслом. Семь из каждых десяти группировок действуют в трех и более стран.

При этом более половины преступников, чья деятельность отмечена в Евросоюзе, не являются его гражданами. Это в основном выходцы из Восточной Европы и Северной Африки.

Авторы доклада обращают внимание на рост уровня насилия в 2021 году, что, по их мнению, отражает усиление конкуренции внутри криминального мира за контроль над определенными территориями и сетями. Насилие выражается в формах угрозы, шантажа, запугивания, вандализма, избиений и пыток, похищений, убийств.

Как и легальная экономика, криминальный бизнес не избежал воздействия пандемии Covid-19, связанной с ней рецессии и упадка. В определенном смысле, отмечает доклад Европола, преступники воспользовались новой реальностью для достижения своих целей. Они смогли быстро капитализировать страхи и неуверенность населения для продвижения как нелегальных, так и легальных остродефицитных продуктов, имеющих жизненное значение во времена эпидемии.

Стефано Сиджиа, старший консультант бельгийской компании Pideeco (консалтинг и торговля в сфере коммуникаций) отмечает, что сицилийская Коза Ностра, неаполитанская Каморра и другие криминальные мафиозные организации широко пользуются трудным экономическим положением, в котором из-за пандемии оказались многие предприятия и бизнесы в этой стране. Особенно в сфере малого и среднего

бизнеса. Оказавшимся на грани банкротство компаниям мафиози предоставляют небольшие кредиты в обмен на отмывание грязных денег.

*(о ситуации с криминалом в развивающихся странах читайте в следующем выпуске журнала)*