**Охрана предприятия**

**№1 (77), 2021**

**Оглавление**

**«Карьерные хакеры»: спрос на них растет**

*Книжное обозрение*

**Red Team: How to Succeed by Thinking Like the Enemy**

# Коронавирус и физическая охрана

До эпидемии коронавируса главными угрозами для бизнеса считались терроризм, инсайдерство, стихийные бедствия, пишет журнал Security Magazine, December 1, 2020. В принципе эти угрозы сохранились и в 2020 году. Однако пандемия COVID-19 существенно скорректировала задачи, стоящие перед корпоративными службами безопасности.

Говорит Кейт Оринжер, руководитель охранного предприятия Security ProAdvisors, специализирующегося в сегменте слияний и присоединений: «Связанный с пандемией кризис экономики затронул много охранных фирм. Существенно упали доходы в этой индустрии. Кризис расширил возможности найма наиболее квалифицированных кадров для физической охраны, но при этом возникла необходимость обучать их новым инструкциям и процедурам, обеспечивать средствами индивидуальной защиты от вируса». Кроме того, добавляет Оринжер, перевод работников на «удаленку» потребовал большей координации между руководителем корпоративной службы безопасности и специалистами в области кибербезопасности, искусственного интеллекта, систем распознавания лиц и прочих высоких технологий.

На фоне общей тенденции к сокращению числа постоянных сотрудников СБ в отдельных случаях возникает потребность в дополнительных охранниках. К примеру, юридический факультет техасского университета (Texas A&M University School of Law), отвечая на требования соблюдать санитарную дистанцию, вынужден арендовать для лекций и семинаров более просторное помещение - конференц-зал в расположенном по соседству отеле. Соответственно пришлось увеличить число охранников. Были закрыты входы в главное здание, за исключением центрального, но одновременно усилен внутренний контроль за тем, чтобы лифтом могли пользоваться не более двух человек, а все находящиеся в здании носили маски. Соблюдение санитарных предписаний легло на плечи охраны.

Временная приостановка производства и бизнеса также потребовала от охранных предприятий новых подходов. Если ранее, до эпидемии, усиленная охрана зданий и помещений велась в рабочие часы, а в остальное время суток можно было обойтись одним-двумя охранниками, то сегодня многие закрытые на карантин офисы требуют круглосуточной и серьезной защиты от мародеров, грабителей и прочих злоумышленников, пользующихся моментом.

Обычно охранное предприятие опирается на помощь клиентской организации, с персоналом которой проводятся специальные тренинги по безопасности. С переводом работников на дистанционную работу «ушей и глаз» заметно поубавилось, что прибавило забот охране.

Экономический кризис повлиял на сферу слияний и присоединений охранной индустрии. Обостряется конкуренция между крупными корпорациями и фондами прямых инвестиций за поглощение малых охранных предприятий, испытывающих потерю клиентов, нехватку финансовых средств. Крупные акулы охранного бизнеса заметно активизируют экспансию в международном масштабе. В первую очередь это относится к американским корпорациям.

Другой вектор наблюдаемой экспансии – технологический. Речь идет о тенденции поглощения производителей и поставщиков технологий безопасности корпорациями – пользователями, т.е. охранными предприятиями. Последних особенно интересуют разработчики и производители систем кибербезопасности, искусственного интеллекта, распознавания лиц, видеонаблюдения, программных решений для интеграции физических и цифровых средств охраны.

# Как коронавирус повлиял на приоритеты охранной деятельности

Исследовательская и консалтинговая компания IDG провела опрос 522 профессионалов в сфере корпоративной безопасности из Северной Америки, Европы и Тихоокеанского региона. Задача опроса – изучить, как эпидемия коронавируса повлияла на управление рисками и угрозами для бизнеса. Основные выводы отчета опубликовал журнал Chief Security Officer, December 1, 2020.

Когда компании были вынуждены отправить на дистанционную работу всех или часть своих сотрудников, мир криминала немедленной воспользовался этим. Опрос показал, что за последний год 36% инцидентов безопасности представляли собой фишинговые атаки с задачей овладеть корпоративными базами данных. Злоумышленники при этом не без оснований рассчитывают на бреши в информационной защите, возникающие при массовом переводе людей на «удаленку». И действительно, треть инцидентов обусловлена вовремя не залатанными дырами в системах кибербезопасности, нарушенными конфигурациями сетевой инфраструктуры. При этом эксперты не знают, как обнаруженные уязвимости дали бы о себе знать в нормальных условиях, без эпидемии.

Компании вынуждены подстраивать технологии и защитные системы к новым угрозам. Но и киберкриминал не бездействует, постоянно меняет тактику в поисках слабых мест. В результате компании пересматривают свою стратегию оценки рисков и реагирования. 62% респондентов опроса IDG заявили о необходимости коренным образом обновить свой подход к анализу угроз и рисков.

Большинство (87%) признают, что их организации недорабатывают в противодействии новым угрозам. 31% считают, что службы кибербезопасности плохо финансируются. Каждый третий респондент указывает на то, что производители интернет приложений недостаточное внимание уделяют вопросам безопасности. 25% полагают, что пользователи корпоративных сетей и интернета мало тренируются.

Отвечая на вопрос, что делать для успешной минимизации рисков, большинство считают необходимым увеличивать число специалистов по кибербезопасности в

каждой отдельно взятой организации. 38% видят решение в увеличении расходов для адекватного реагирования на инциденты кибербезопасности. 30% предпочитают больше внимания уделять модернизации защитных технологий и планам обеспечения непрерывности бизнеса (business continuity).

Как эпидемия коронавируса повлияла на бюджеты корпоративных служб безопасности?

Эксперты обнаружили, что планируемые организациями бюджеты на период после эпидемии не обязательно означают увеличение расходов на корпоративную безопасность. Хотя 41% респондентов ожидают увеличения финансирования в 2021 году, только 33% связывают такие ожидания с коронавирусом. Напротив, каждый четвертый из опрошенных специалистов полагает, что бюджеты на безопасность будут урезаны из-за пандемии. Примерно половина респондентов надеются, что финансирование сохранится на прежнем уровне.

Безотносительно того, как будет финансироваться корпоративная безопасность в ближайшие годы, наиболее расходную статью составит персонал (23% выделяемых средств - на штатных работников, 8% - на аутсорсинг). Остальная часть бюджета распределяется между программным обеспечением, модернизацией систем безопасности, облачными вычислениями и прочими технологиями.

Что касается технологий безопасности, то наиболее перспективными в ближайшие годы эксперты считают следующие:

*Принцип «нулевого доверия»*

Еще до начала мировой пандемии многие организации уже присматривались к такой модели (модель «нулевого доверия» исключает запуск любого процесса или операции, которой вы не доверяете с точки зрения потенциальных рисков). Коронавирус заставил практически рассматривать включение принципа «нулевого доверия» в стратегию и тактику безопасности. 28% опрошенных сказали, что уже используют этот принцип или планируют пилотный проект в течение ближайшего года. 40% изучают данный принцип и вскоре примут решение.

*Сетевые ловушки и приманки*

Такие технологии предназначены, чтобы обманывать хакеров, заманивая их в фальшивые псевдо сети и фиктивные базы данных, которые злоумышленники принимают за настоящие. Такие ловушки помогают не только отводить удар, но и знакомиться с приемами и способами, используемыми киберкриминалом. Треть респондентов заявили, что изучают подобные приманки для практического применения.

*Политики и инструменты аутентификации*

С переводом людей на «удаленку» их значение резко возросло. Организации стали чаще использовать мультифакторную и ролевую виды аутентификации. 32% участников опроса подтвердили стремление вкладывать средства в такие решения в 2021 году.

*Аутсорсинг*

Из-за пандемии коронавируса аутсорсинг выдвинулся в число наиболее значимых приоритетов информационной защиты. Это связано как с необходимостью экономить средства, так и с ожидаемой эффективностью от облачных вычислений. 22% опрошенных заявили о планах переноса в «облака» систем защиты информации и мониторинга безопасности. Также на аутсорсинг передаются функции тестирования и оценки надежности систем физической охраны и кибербезопасности, аудита.

# Лидерские качества для успешной карьеры в охранной индустрии

Многие организации обладают сложными процессами и структурой, пишет постоянный автор журнала Security Magazine Джерри Бреннан в ноябрьском выпуске. Значение персональных, личностных характеристик работающих в них менеджеров, в том числе влияющих на взаимоотношения с подчиненными и коллегами, трудно переоценить. Если у вас сильно развитое собственное эго, если ваша личная карьерная повестка не настроена на задачи, которые вы должны решать как руководитель службы безопасности, то проблемы неизбежны. И напротив, твердые этические принципы, уважение к коллегам способствуют профессиональному, карьерному росту.

Бреннан перечисляет требования, важные для успешной работы организации и личной служебной карьеры:

- Ищите, привлекайте и развивайте таланты. Вы должны правильно оценивать значение способных, талантливых кадров для успешного бизнеса.

- Всячески способствуйте профессиональному росту членов своей команды. Создавайте условия для развития их стратегического мышления, креативности. Не держите профессионалов в одном узком сегменте служебной вертикали, но обеспечивайте возможность выхода на разные мультифункциональные задачи, поощряйте инициативы и желание продолжать учебу, повышать квалификацию.

- Контролируйте свое эго. В разумных пределах оно, конечно, полезно и даже необходимо как фактор здорового честолюбия. Но раздутое самомнение, нарциссизм играют деструктивную роль, не могут рассматриваться как положительные качества.

- Воспитывайте и развивайте врожденную любознательность, склонность не стандартно, творчески мыслить, равно как и умение внимательно слушать.

- Поощряйте открытый диалог, свободное обсуждение.

- Продвигайте упреждающие способы решения проблем. Вы должны научиться предвидеть последствия проблем, прежде чем они появятся на экране монитора.

- Ищите и набирайте в команду людей с самостоятельной и достаточно независимой точкой зрения. Избегайте рабских исполнителей ваших указаний или тех, кто во всем пытается имитировать вас.

- Не забывайте, что и ваши познания, компетенции в чем-то ограничены. Приглашайте

специалистов, способных компенсировать недостатки.

- Люди в той или иной степени эмоционально чувствительны. Проявляйте к ним уважение. В противном случае вам не стать настоящим лидером.

- Проявляйте личную ответственность не только за успехи, но и за ошибки, неверные решения, неосторожные слова, которые чреваты нежелательными последствиями.

Джерри Бреннан объясняет, что сформулированные им требования необходимы именно для руководителя службы безопасности, поскольку в отличие от некоторых других функций организации программа охраны и безопасности затрагивает и поддерживает буквально «каждый угол» в компании. Эта особенность охранной функции требует от руководителя желания и способности схватывать и учитывать главные драйверы бизнеса, мыслить широко и стратегически в масштабах всей организации.

# Цифровая трансформация в охранной индустрии и искусственный интеллект

Массовый переход людей на дистанционную работу, считают эксперты, подхлестнул процесс цифровой трансформации практически всех отраслей экономики и бизнеса, включая охранную индустрию. Одним из проявлений этой тенденции является концентрация внимания аналитиков безопасности на мониторинге социальных сетей в качестве важнейшего ресурса для поиска и обнаружения потенциальных угроз.

Отслеживание чатов и блогов может принести для «разведки безопасности» (security intelligence) неожиданные результаты, например, обнаружить ранние признаки потенциальных рисков и угроз бизнесу, утверждают эксперты Челси Биннс, доцент John Jay College of Criminal Justice, и Робин Кемпф, доцент Colorado University. В интервью журналу Security Magazine, December, 2020, они обращают внимание на необходимость отслеживать жалобы и претензии клиентов компании. Если ранее свою озабоченность теми или иными продуктами и услугами люди обычно направляли в адрес организации, то сегодня большинство предпочитают высказывать свое возмущение, недовольство в социальных медиа. Например, тем, что, по их мнению, нарушаются права личности. Или утекают в открытый доступ персональные данные, предоставленные фирме в конфиденциальное пользование.

Отслеживая и анализируя в соцсетях данные, касающиеся одной риелторской фирмы, Биннс обнаружил тревожную тенденцию. Ряд клиентов заявили об атаках хакеров на их аккаунты, зарегистрированные в фирме. Вместо того, чтобы сообщить об этом напрямую в компанию, они написали об этом в Твиттере. «Если вы не удосужились «прошерстить» Твиттер – 100 тысяч сообщений – то у вас никогда не будет полной картины происходящего», - подытоживает Биннс.

Понятно, что вручную, без обращения к автоматическим поисковым машинам, к искусственному интеллекту, такую работу не сделать. В то же время термин «искусственный интеллект» применительно к сфере корпоративной безопасности отнюдь не однозначен, считает М. Кул, главный аналитик School of Science at Edith

Cowan University. «ИИ в последнее время стал расплывчатым, неточным понятием, под которым подразумевается технология, призванная заменить человеческий мозг в работе с большими объемами информации. Однако, это неверная посылка. Компьютеры, даже самые мощные и совершенные, не воспринимают и не понимают широкий контекст. Машины с ИИ способны выполнять многие исследовательские, в том числе разведывательные, задачи, которые решает человек, помогают добиваться существенных результатов. Но они не могут воспроизводить процессы, происходящие в человеческом мозгу, а потому лишены того, что можно определить как «метопознание» (meta-cognition) или «метаосведомленность» (meta-awareness). Существуют принципиальные различия между тем как компьютер и человек обрабатывают, анализируют информацию. Поэтому прямолинейные аналогии между ИИ и человеческими способностями порождают множество недоразумений» (Security Magazine, December, 2020).

М. Кул формулирует три основные категории искусственного интеллекта.

*Узкий ИИ*. Компьютерная способность решать конкретные, очень специфические задачи.

*Широкий ИИ*. В комбинации с «узким ИИ» может осуществлять определенные бизнес процессы, например, управление беспилотным автомобилем.

*Генеральный ИИ*. Владеет способностями, которыми наделен человеческий мозг, в том числе, самопознание, способность переживать чувства, такие как вера, ожидания, эмоции… Эта категория относится к далекому будущему, считает эксперт.

Сегодня же, по его мнению, программные продукты с ИИ применительно к сфере корпоративной безопасности представляют собой комбинации «узкого ИИ» (к примеру, биометрический анализ), с «широким ИИ», решающим, например, задачу - выдать разрешение на доступ или отказать.

Адаптация ИИ к функции безопасности наталкивается на ряд сложных проблем, связанных с операционной совместимостью и трудностями управления. Наиболее успешно такого рода проблемы сегодня решаются в современной армии. В перспективе военный опыт использования ИИ будет перенесен в область гражданского применения, уверен Кул.

Искусственный интеллект помогает человеку вскрывать тенденции, принимать просчитанные решения. Но сам по себе, без человека, ИИ весьма ограничен в своих возможностях.

# Технологии распознавания лиц в условиях масочного режима

Введение масочного режима как самого простого и массового противовирусного средства защиты поставило под вопрос эффективность использования технологии распознавания лиц в сфере безопасности, как государственной, так и корпоративной.

Об этой проблеме пишет журнал Security Management, November, 2020, оперируя результатами тестирования технологий распознавания лиц, которые регулярно, на протяжении многих лет, проводит U.S. National Institute of Standards and Technology (NIST). По данным последнего тестирования, осуществленного летом 2020 года, зарекомендовавшие себя наилучшим образом коммерческие алгоритмы, допустимая погрешность которых в обычное время не превышает 5%, ошибаются в 20 - 50% случаев при совмещении фото человека с его изображением в маске. Всего в тестировании участвовали 89 разных технологий распознавания лиц.

При этом отмечено, что на точность идентификации влияет размер, конфигурация и даже цвет маски. Бледно-голубые маски порождают меньше ошибок, чем черные. Маски, покрывающие большую часть лица, например, хирургические, дают больше ошибок. Особенно те, которые полностью закрывают нос. Именно нос имеет ключевое значение при распознании: нижние маски увеличивают эффективность идентификации в пять раз сравнительно с высокими (т.е. покрывающими нос) масками.

Конечно, нельзя считать результаты исследования абсолютно достоверными.

Во-первых, тестирование проводилось не с реальными, живыми персонажами, а с их цифровыми фотографиями. Всего было использовано несколько миллионов фотографий из архивов пограничной службы.

Во-вторых, на этих фото глаза смотрели в камеру, в то время как в реальности люди, как правило, движутся под определенным углом к видеокамере, что, естественно, влияет на точность.

В-третьих, надо принимать во внимание, что протестированные алгоритмы были выпущены до начала пандемии, когда о грядущем масочном режиме никто не подозревал.

Один из авторов исследования, Мэй Нган, эксперт по компьютерным технологиям NIST, отмечает, что технологии некоторых производителей показали большую эффективность распознавания лиц в маске по сравнению с конкурентами. «В ходе тестирования мы не располагали данными о том, учитывали ли производители возможность использования технологий распознавания при ношении масок. Однако конкретные результаты показывают, что некоторые из представленных образцов превосходят другие по эффективности идентификации в условиях пандемии».

Эксперты считают, что адаптация технологий распознавания лиц к новым условиями предполагает смещение фокуса алгоритмов на периокулярную (окологлазничную) открытую область лица. Некоторые разработчики идут по пути создания принципиально новых технологий, ориентированных исключительно на носителей масок.

Что касается пользователей, то эксперты рекомендуют обращаться к провайдерам с требованием внесения улучшений, которые рассчитаны на идентификацию лиц одновременно в масках и без оных. Работы в этом направлении ведутся.

# Сигналы о рисках насилия в учебных заведениях требуют мульти-дисциплинарного подхода

С переводом школ и вузов на полную или частичную «удаленку» определенные изменения претерпевает система сигналов, предупреждающих о возможных актах насилия, отмечает Фрэнк Штрауб, директор Center for Mass Violence Response Studies. «С приходом пандемии условия жизни учащихся и студентов заметно усложнились. На их поведение не могут не влиять такие факторы новой среды как экономическая неопределенность, семейная нестабильность, изоляция, финансовые проблемы – всё, что даже в нормальной жизни может провоцировать потенциально опасные перемены в поведении» (Security Management, 1 November 2020).

Как правило, акту насилия предшествует какое-то происшествие, изменение в личной жизни, полагает Штрауб. Таким изменением может быть развод родителей, семейные финансовые трудности из-за потери работы, иные проблемы, которые влияют на психику, вызывают депрессию. Это непосредственно выражается в понижении социальной активности, чрезмерной реакции на критику, в сознательном отстранении от круга друзей. К примеру, учащийся школы, всегда дружелюбный и компанейский с одноклассниками, вовлеченный в общественные дела, охотно участвующий в спортивных состязаниях, внезапно замыкается в себе, сторонится друзей. В другом случае отмечается беспричинное, на первый взгляд, снижение успеваемости. В третьем случае замечен повышенный интерес к экстремистской идеологии, оружию, фактам стрельбы в учебных заведениях…

«Все эти моменты представляют собой тревожные сигналы об изменении поведения, которые необходимо отслеживать и соответственно реагировать», подчеркивает Штрауб. Задача усложняется, если класс (или вузовский курс ) переведен на «удаленку».

Диана Конкэннон, декан California School of Forensic Sciences, обращает внимание, что реакция руководства на нарушения порядка, даже самые незначительные, со стороны учащихся нередко сводится к чисто административным методам воздействия. Такое реагирование обычно оправдывается желанием предотвратить трансформацию мелких нарушений в насилие. На самом деле это далеко не так, считает Конкэннон: «Молодежи свойственна жизнерадостность. Каждый факт проявления стресса или взволнованности требует к себе внимания, не обязательно с точки зрения угрозы насилия, а просто для поддержки морально-психологического состояния. Но в случае продолжительного характера или серьезности стресса, неподобающего поведения необходимо вмешательство и расследование» (там же).

«Преподаватели не обучены управлению рисками, - продолжает Конкэннон, - К ним попадает тревожная информация, но они не знают, как реагировать. Конкэннон и другие эксперты рекомендуют создавать в каждом учебном заведении междисциплинарную группу с участием представителей администрации, охранного предприятия, отвечающего за безопасность школы или вуза, а также специально обученного «school resource officer», в дословном переводе: «школьного офицера полиции». Это распространенная в США и некоторых других странах должность

наставника молодежи, которая в последние годы трансформировалась в фигуру «полицейского в штатском», который нанимается местными правоохранительными органами для предотвращения беспорядков и случаев насилия, обеспечения безопасности в учебных заведениях.

Последний должен обладать знанием и навыками сбора информации в условиях дистанционного обучения, внимательно анализировать поведение студента (школьника) в онлайновом режиме. Вести расследование в виртуальной учебной аудитории – далеко не то же самое, что расследовать угрозы в реальной, традиционной среде. Важно держать контакт не только со студентом, но и с родителями, администрацией и преподавателями учебного заведения, местной полицией. А, кроме того, и с психиатрами, если необходимо. Такой вот разносторонний специалист, умеющий в отличие от преподавателей своевременно обнаруживать потенциальные угрозы.

Штрауб так формулирует задачу междисциплинарной команды: «выявить как можно быстрее признаки тревоги и беспокойства, в которых пребывает школьник или студент, наладить с ним/ней контакт с целью выяснить причины такого поведения, разработать и осуществить план помощи в решении проблемы».

# Сетевое взаимодействие транспортных средств: плюсы и минусы с точки зрения кибербезопасности

Новые автомобили все более напоминают компьютеры на колесах. В распоряжении водителей огромное количество электронных контроллеров, включая датчики давления шин, съезда с полосы движения, состояния тормозов. Промышленники предлагают мобильные приложения, позволяющие диагностировать неисправности, автоматически закрывать двери, определять местонахождение машины (если водитель забыл, где припарковался) – и все это осуществлять через персональный смартфон.

Очевидные преимущества информационных технологий генерируют одновременно рост киберугроз, пишет Мигэн Гейтс в журнале Security Management, November, 2020. В 2018 году исследовательская группа компании 360 Group (международная рекламно-консалтинговая фирма, представленная в России) обнаружила уязвимость в автомобиле Мерседес-Бенц Е-класса, позволявшую умелым хакерам снимать сигнализацию, отпирать двери и включать двигатель. Экспертная группа Black Hat 2020 в ходе тестирования получила несанкционированный контроль над компьютерной сетью автомобилей, о чем и доложила руководству компании Мерседес.

В другом случае американские эксперты по кибербезопасности успешно взломали компьютер Jeep Grand Cherokee, что вынудило ФБР выпустить специальное предупреждение (Private Industry Notification - PIN) об уязвимостях электронных дивайсов в автомобильной индустрии, которые несут реальную угрозу безопасности.

Еще ранее от владельцев грузового транспорта в Америке потребовали установить

систему электронных записей (electronic logging device – ELD), которая автоматически, в режиме реального времени, передает в комиссию по транспортной безопасности (Federal Motor Carrier Safety Administration - FMCSA) дату, время и локацию автомобиля, а также идентификационную информацию об автомобиле и его владельце/водителе, пробег в километрах и часах работы двигателя, номер двигателя.

Однако, производители электронных регистраторов, отмечают эксперты, зачастую пренебрегают требованиями безопасности. В результате беспроводное сетевое взаимодействие уязвимо перед атаками хакеров. Несанкционированное вторжение в эти коммуникации открывает перед злоумышленниками возможности овладеть персональными данными, пролезть в корпоративную сеть транспортной компании, вывести из строя компоненты управления автомобилем.

До 16 декабря 2019 года установка ELD носила рекомендательный характер, после – обязательный. Но при этом никто из федеральных органов США не озаботился серьезно о том, чтобы система была безопасной.

Хотя специалисты считают маловероятным, что хакеры будут тратить время и силы на компрометацию систем отдельного грузовика, нельзя исключать их повышенный интерес к транспортным средствам, перевозящим отравляющие и прочие опасные химические вещества, считает Дуг Моррис, директор по вопросам безопасности общественной организации Owner-Operator Independent Drivers Association – OOIDA. По словам Морриса, эта ассоциация, представляющая интересы 160 000 владельцев и водителей транспортных средств, постоянно обращается к законодателям разных уровней с требованием принять законы и нормы, ужесточающие требования к кибербезопасности электронных систем коммуникации на транспорте. В противном случае, подчеркивает он, не исключены серьезные сбои, негативно воздействующие на функционирующие цепочки поставок.

Моррис говорит о множестве жалоб водителей грузовиков на проблемы в измерительных приборах и датчиках, которые они связывают с установкой ELD. А когда ассоциация OOIDA обращается напрямую к производителям и поставщикам систем электронных записей, то те уходят в кусты. «Мы не можем склонить промышленников к откровенному, честному разговору. Стремясь любой ценой «впарить» свой продукт, они говорят лишь то, что клиент хочет услышать, но не всю правду», - сетует Моррис.

Он также критикует и федеральное ведомство по транспортной безопасности (FMCSA), которое, по его словам, вместо того, чтобы принимать реальные меры по обеспечению кибербезопасности, например, установить жесткие технические стандарты для ELD, внедрить лучшие практики тестирования и проверки на безопасность, рассылает водителям и владельцам автотранспорта уведомления, напоминания, рекомендации и прочие малозначащие бумажки.

# Центры управления корпоративной безопасностью во время пандемии

Син Гарсия, один из руководителей компании Sureview (платформы охранной

сигнализации и видеонаблюдения на базе IP), провел неформальный опрос среди клиентов относительно воздействия пандемии на охранную деятельность, конкретно – на работу центров управления и реагирования на инциденты. Клиентская база Sureview охватывает как транснациональные корпорации со штатом в сотни тысяч работников, так и малые предприятия, служба безопасности которых осуществляет локальные операции, в пределах студенческого кампуса или одного здания.

Свои выводы и соображения он опубликовал в интернет издании Security Magazine, October 19, 2020.

Общий итог – все без исключения службы корпоративной безопасности вынуждены вносить изменения в процессы охраны, и этот тренд будет сохраняться в обозримом будущем. К примеру, в одной крупной компании заболел коронавирусом сотрудник центра управления охраной. Немедленно все, кто с ним контактировал, были переведены на дистанционную работу. В другой организации в целях мониторинга и контроля за здоровьем работников была введена в действие специальная программа («track-and-trace»), потребовавшая заново переписать политики и инструкции по охране. В третьем случае технологии видеоаналитики были приспособлены для измерения температуры тела в местах интенсивного движения сотрудников компании – при входах в здание, в столовую и т.п.

Приведенные примеры демонстрируют высокую вариантность реагирования на кризис. Выбор пути зависит от приоритетов компании, ее месторасположения, окружающей среды, требований регуляторов, прочих разных условий. Тем не менее, Гарсия выделил и сформулировал ключевые требования, соблюдение которых облегчает задачи быстрого реагирования на возникающие в связи с пандемией проблемы и соответствующей перестройки охранных операций.

*Гибкость, необходимая для дистанционного управления операциями*. В случае заболевания одного члена команды, перевод остальных на «удаленку» должен проходить безболезненно для работы службы безопасности.

*Способность оперативно формулировать и внедрять новые инструкции и политики*, которые соответствуют быстро меняющимся условиям работы.

*Максимальное внимание к обеспечению коллективной, командной работы*. Это критически важно, когда многие работники переводятся на дистанционную работу.

*Стандартизация способов и путей получения информации о здоровье работников*.

*Всегда помнить о необходимости строго следовать инструкциям и рекомендациям по итогам аудитов и проверок.*

*Отдавать предпочтение сравнительно простым технологически системам видеонаблюдения*, поскольку сегодня уже мало кто может позволить себе роскошь тратить огромные деньги на приобретение дорогостоящего оборудования и многие месяцы на их установку и обкатку. Так как все организации в той или иной степени переживают кризис, SureView Operations выпустило гибкую «облачную» платформу для видеомониторинга, которую компании любого размера могут развернуть в сжатые сроки и управлять ею дистанционно, добиваясь максимально быстрого и эффективного реагирования на инциденты.

# Организация служебных поездок во время пандемии

Эпидемия коронавируса обвалила сферу туризма и путешествий, в том числе и служебных командировок. Согласно опросу, проведенному Global Business Travel Association (GBTA) среди 1380 компаний разных стран, 92% организаций отменили в 2019 году или перенесли запланированные международные командировки на более поздний срок, 70% были вынуждены сделать то же самое в отношении поездок внутри своих стран.

«Это новая реальность», с грустью констатирует Николь МакДаргх, региональный директор по безопасности в Европе корпорации Richemont (производство предметов роскоши). С началом пандемии большинство сотрудников корпорации были переведены на «удаленку». Все поездки на ближайшие месяцы были отменены (Security Management, 1 December 2020).

По мере постепенного оживления бизнеса в промежутке между первой и второй волнами пандемии многие организации вернулись к планированию служебных поездок, внося в подготовку существенные коррективы. На первом месте – учет ситуации с коронавирусом на местах. Правила, регулирующие ограничения на передвижение, различаются не только от страны к стране, отмечает МакДаргх, но и между внутренними регионами. Причем они постоянно меняются, добавляет она.

Радек Гавлис, руководитель управления безопасности консалтингового гиганта PricewaterhouseCoopers (PwC) по Восточной Европе и Центральной Азии, обращает внимание на необходимость отличать важные командировки от менее значимых. Руководствуясь этим подходом, корпорация PwC отменила до конца 2020 года все командировки, признанные малозначимыми.

Бизнесмены должны тщательно оценивать потенциальные последствия, принимая решение о поездке - своей или подчиненных, подчеркивает Гавлис. К примеру, компания во имя сохранения здоровья и жизни работников решает на время запретить любые служебные командировки. С одной стороны, она защищает себя от возможных претензий и жалоб в случае заражения во время поездки, тем более, летального исхода. С другой стороны – налицо риск потерять клиентов и партнеров, чреватый большими убытками и неизбежными в этом случае увольнениями. Выбор непростой, требующий кропотливого анализа в поисках единственно правильного баланса, продолжает Гавлис.

Николь МакДаргх рекомендует при планировании командировок внимательно изучать и отслеживать антивирусные ограничительные меры, которые предпринимаются в странах назначения, используя официальные источники информации этих стран, не в последнюю очередь – сайты департаментов здравоохранения в отдельных регионах. По прибытии на место командировки необходимо поставить в известность о своем приезде местные власти и соответствующий орган здравоохранения.

Гавлис дополняет, что программа поездки должна предусматривать предварительную договоренность с клиентом/партнером относительно социальной дистанции и индивидуальных средств защиты во время переговоров. Если в ходе очной встречи

командированный не чувствует себя достаточно защищенным, компания должна прервать переговорный процесс, чтобы уточнить, насколько верно контрагент выполняет предварительные договоренности о мерах защиты. И затем решить, стоит ли продолжать контакты.

К сожалению, для большинства людей риск представляется как нечто абстрактное, отмечает Мередит Мур, основатель и глава компании Greylake Training Solutions, организующей специальные тренинги по безопасности поездок. Они склонны игнорировать требования защиты от вируса в рутинных поступках и действиях, находясь вдали от дома и места постоянной работы. Легкомысленный настрой затрудняет психологическую подготовку к возможным проблемам и трудностям во время командировки. «Неимоверно трудно заставлять людей ломать стереотипы, менять свое поведение» (там же).

Мур рекомендует проводить подготовительные тренинги не стандартно. В какой бы форме занятия ни проводились – письменные тесты, виртуальные задания, погружение в реальность страны назначения – не следует полностью фокусировать внимание на потенциальных угрозах и рисках. Желательно сконцентрироваться на вопросах психологической подготовки к проблемам и трудностям, которые, возможно, возникнут в ходе поездки.

По мнению Мур, целесообразно использовать принцип «одного окна» - обеспечить командированного цифровым приложением, которое содержит все необходимые указания, рекомендации и контакты. Одним приложением легче управлять.

Помимо ментального аспекта тренинг помогает в чисто практическом плане разобраться, какие медицинские справки необходимы для пересечения границы, с кем из офиса держать постоянный контакт, какие сценарии развития ситуации наиболее характерны для страны пребывания и как на них реагировать.

По мнению большинства экспертов, санитарные требования для командированных сохранятся как минимум ближайшие три года, вне зависимости от того, насколько успешной будет массовая вакцинация от коронавируса.

# Охранная индустрия в Азии

Журнал Security Management продолжает публикацию материалов о состоянии и перспективах охранной индустрии в разных регионах мира. В ноябрьском номере издания предлагается интервью с К.А. Лью – директором восточноазиатского отделения Глобальной службы безопасности корпорации Johnson & Johnson с офисом в Шанхае. Приоритетная задача его команды – защита бренда компании, борьба с контрафактом и нелегальной торговлей под прикрытием имиджа всемирно известной фармацевтической организации. В его послужном списке – 7 лет работы в правоохранительных органах Китая плюс охрана цепочек поставок ряда транснациональных корпораций в Восточной Азии.

Лью отвечает на вопросы Security Management:

*Как Ваш предыдущий опыт помогает эффективно решать задачи, стоящие перед*

*региональным отделением Глобальной службы безопасности в корпорации Johnson & Johnson?*

Служба в силовых структурах вырабатывает чувство профессиональной добросовестности и честности, помогает приобретать навыки, необходимые для определения приоритетов и эффективного управления множеством задач, развивает коммуникативные способности, придает уверенность в своих силах. Работа в частном бизнесе способствует лучшему пониманию особенностей технологий безопасности, призванных минимизировать риски, а также тесной взаимозависимости охранной функции и профильного бизнеса.

*С какими вызовами сегодня сталкивается в Азии охранная индустрия?*

Во-первых, диверсифицированная культура. Работая на международном уровне, нельзя забывать, что один и тот же подход к решению задачи в одних странах воспринимается нормально, в других вызывает отторжение.

Во-вторых, различия в структуре и характеристиках угроз и рисков на азиатском континенте. Стандарты безопасности, подходящие для одних стран, могут быть малоэффективными для других.

В-третьих, и это главное: понимание бизнес стратегии компании, в которой вы работаете. Деловая среда меняется от страны к стране, причем довольно динамично. Важно быстро идентифицировать и анализировать совершенно разные по характеру риски, свойственные рынкам стартапов, развивающихся и развитых экономик. Все эти рынки представлены в Азии.

*С точки зрения рисков и угроз, с которыми приходится повседневно иметь дело, в чем особенности работы и жизни управленца по корпоративной безопасности в Шанхае? С какими конкретно вызовами Вы сталкиваетесь каждый день? Какие угрозы Вас беспокоят больше всего?*

Мой рабочий день в основном связан с реагированием на инциденты. К примеру, я обсуждаю с акционерами компании вопросы контрафакта наших приоритетных брендов, взаимодействия с местными правоохранительными органами в подаче исков в суд. Провожу проверку систем физической охраны офисов и складов. Организую инвентаризацию хранящейся на складах продукции. Осуществляю аудит безопасности по всей цепочке поставок, включая анализ рисков информационных утечек. Занимаюсь организацией безопасности приезжающих в регион менеджеров компании. Участвую в расследовании инцидентов, связанных с охраной служебных секретов. Часто выезжаю на места.

Наибольшую озабоченность вызывает рост онлайновых угроз на фоне расширения практики аутсорсинга и внедрения интернет технологий, в том числе облачных вычислений .

*Как в Шанхае и Китае в целом выстраиваются взаимоотношения между рядовыми работниками и их менеджерами? Как меняется производственная культура?*

Последние 20 лет благодаря воздействию транснациональных компаний внутрикорпоративная культура существенно изменилась. Все шире применяются практики «открытого рабочего пространства» (open workplace), способствующие

самоорганизации, повышению ответственности за вклад и результат каждого участника.

*Претерпевает ли изменения охранная функция в китайских компаниях?*

Да. Меняется в двух аспектах.

Во-первых, происходит расширение функции, когда помимо традиционной физической охраны охватываются такие сегменты корпоративной безопасности как расследования, кризисное управление, безопасность служебных поездок и так далее… В этом сказывается влияние международных компаний, пришедших в Китай.

Во-вторых, корпоративные службы безопасности в Китае претерпевают тактические изменения, что выражается в перенесении приоритетов с реагирования на инциденты на уровень стратегии, когда основной упор делается на предотвращение инцидентов, минимизацию потенциальных рисков и угроз.

# Евросоюз: новые требования к финансовым институтам относительно управления киберрисками

Осенью 2020 года опубликован законопроект Евросоюза, налагающий на банки и прочие финансовые организации, действующие на территории стран Евросоюза, более жесткие требования к работе с рисками и угрозами.

Этот законопроект, получивший название Digital Operational Resilience Act (DORA), рассматривается как часть «Цифровой финансовой стратегии», разрабатываемой Евросоюзом последние два года. Он охватывает абсолютно все финансовые институты – от банков до инвестиционных фондов и покрывает следующие сферы деятельности:

*Управление рисками*. Компании обязывают: а) устанавливать и эксплуатировать устойчивые информационно-коммуникационные системы и инструменты, способные минимизировать риски на постоянной основе; б) внедрять меры защиты и предупреждения инцидентов кибербезопасности; в) разрабатывать планы выживаемости и восстановления бизнеса в условиях форс-мажора.

*Отчетность об инцидентах.* Финансовые организации должны разрабатывать и строго следовать четким инструкциям по вопросам мониторинга, классификации и отчетности перед соответствующими компетентными инстанциями о всех значимых инцидентах кибербезопасности.

*Тестирование цифровых операционных систем*. На компании налагаются обязательства регулярно тестировать возможности и функции, заложенные в цифровых информационно-коммуникационных технологиях, с целью обнаружения уязвимостей, изъянов, пробелов.

*Риски третьей стороны*. Организациям предписано изучать, отслеживать и

документировать риски, связанные с деятельностью партнеров, клиентов, предусматривать в контрактах обязательства третьих сторон соблюдать требования, вытекающие из данного законодательства.

*Обмен информацией*. Законопроект обязывает финансовые организации обмениваться между собой информацией о киберугрозах.

Комментируя законопроект, Фархад Шаудри, главный информационный директор State Street Corporation (американская холдинговая компания, осуществляющая депозитарную и инвестиционную деятельность), полагает, что новый закон повлияет на финансовый сектор Евросоюза в целом и на отдельные организации в зависимости от их размера и оснащенности системами информзащиты.

Майк Батлер, независимый консультант по стартапам, уверен, что DORA окажет минимальное влияние на большинство крупных банков, стратегия и практика безопасности которых уже совпадает с требованиями законопроекта. Что же касается средних и небольших банков, страховых компаний, различных фондов, то многим из них, считает эксперт, предстоит скорректировать свои стратегии и бюджеты в пользу выделения средств на более совершенные технологии.

Эксперты обращают внимание на раздел документа, относящийся к взаимоотношениям с третьей стороной, с партнерами. Здесь, по их мнению, - наиболее слабое звено в системе информационной защиты. Между тем, актуальность безопасности партнерства возрастает по мере того, как набирают популярность аутсорсинг и облачные вычисления. Все виды взаимодействия с партнерами и клиентами должны охватываться периметром кибербезопасности.

В то же время Антон Коноплев, основатель и глава фирмы Palma Violets Loans, предупреждает, что новый закон, ужесточающий правила цифровой безопасности для финансовых организаций, может внести сумятицу и хаос относительно существующих контрактных обязательств, вызвать рост цен на услуги третьих сторон.

Законопроекту DORA предстоит пройти слушания и утверждение в Европарламенте. Такая процедура занимает обычно от 18 до 24 месяцев.

*(по материалам журнала Chief Security Officer)*

# Безопасность футбольного клуба

Спортивный клуб Atlanta United присоединился к профессиональной футбольной лиге Major League Soccer (высшему дивизиону в США и Канаде) сравнительно недавно – в 2017 году. Но уже на следующий год завоевал Кубок Лиги. Домашние матчи команда проводит на собственном стадионе Mercedes-Benz Stadium.

Скотт Эшворд, директор службы безопасности клуба, до прихода в большой спорт 10 лет служил офицером полиции, занимался криминальными расследованиями, обладает дипломом бакалавра по уголовному праву.

В интервью журналу Security Magazine (August 5, 2020) он отмечает, что в Atlanta United, в отличие от других футбольных команд Америки, много иностранных игроков: «Это для нас настоящий вызов, поскольку наличие иностранных легионеров и, соответственно, зарубежных болельщиков, существенно влияет на ландшафт безопасности. Тем более, что ряд игроков хорошо известны и пользуются поддержкой фанатов далеко за пределами США – в Мексике, Центральной и Южной Америке».

Возглавляя службу охраны, Эшворд исходит из того, что вопросы безопасности касаются каждого, кто причастен к футболу, – от болельщиков до владельцев спортивного клуба.

Для измерения эффективности службы Эшворд использует две основные метрики. Первая из них относится к восприятию безопасности самими болельщиками. Среди них регулярно проводятся опросы с целью выяснить, насколько комфортны для них охранные технологии и принимаемые меры безопасности. Здесь важно соблюсти правильный баланс, чтобы каждый, кто приходит посмотреть матч, чувствовал себя и защищенным, и желанным гостем одновременно.

Другая метрика – самоконтроль и самопроверка. «Мы регулярно приглашаем внешних специалистов для объективной, непредвзятой оценки нашей работы по обеспечению безопасности спортивных мероприятий».

Когда Эшворд заступил на нынешнюю должность в 2017 году, служба безопасности (как и клуб в целом) еще формировалась, корпоративные политики и инструкции приходилось формулировать с чистого листа. Особое внимание было уделено плану обеспечения безопасности во время выездных игр. «Был подготовлен подробный план мероприятий по защите игроков, администрации и сопровождающих команду болельщиков. Планом, в частности, предусматривается предварительный выезд в места проведения матчей, установление контактов с местными властями, полицией, органами МЧС, администрацией стадиона, где предстоит играть, отелем, где команда должна остановиться».

Важную роль играют контакты с болельщиками. «Всякий раз, когда нам нужно распространить предупреждение, любую иную информацию, клубные фаны рады помочь. Мы, в свою очередь, открыты для них, всегда готовы разъяснить значение мер безопасности, помочь, когда они в этом нуждаются».

Другой эффективный инструмент коммуникации – социальные сети. Взяв на вооружение современные интернет технологи, СБ внимательно отслеживает хэштеги и аккаунты не только игроков, но всех, кому не безразлична команда, на предмет обнаружения и анализа потенциальных рисков и угроз.

Залог успеха, подчеркивает Эшворд, в заблаговременном планировании. За неделю до проведения домашней игры служба безопасности клуба проводит консультации с управлением полиции города Атланта, городской пожарной частью, представителями регионального и федерального бюро расследований, министерства национальной безопасности. «Каждое из этих ведомств играет ключевую роль в обеспечении безопасности в день игры. Мы встречаемся и обсуждаем детали плана безопасности, проблемы, которые могут возникнуть в преддверии и после игры, фокусируем внимание на мерах предотвращения возможных инцидентов». В день игры Эшворд старается быть поближе к игрокам, чтобы они чувствовали себя в полной безопасности.

Mercedes-Benz Stadium оснащен современной технологией мониторинга. «В нашем распоряжении мощная сеть видеокамер, сильная команда охранников, поддерживающих должный порядок как на территории стадиона, так и на ближних подступах».

# «Карьерные хакеры»: спрос на них растет

Исследовательский институт ITMOAH выпустил доклад «Inside the Mind of a Hacker 2020», посвященный нынешнему состоянию и перспективам легального хакерства. Об основных выводах доклада пишет А. Гупта в журнале Security Magazine, October 15, 2020.

Термин «хакер» изначально носит негативный оттенок. Однако сегодня такой подход уже не актуален. Авторы исследования провели опрос трех с половиной тысяч т.н. «добропорядочных хакеров», предлагающих компаниям легальные услуги в деле противодействия киберкриминалу. Число таких «карьерных» хакеров увеличивается быстрыми темпами соответственно растущему спросу. Эпидемия коронавируса подхлестнула отмечаемую тенденцию.

Опрошенные хакеры считают наиболее уязвимой для киберкриминала сферу здравоохранения. На втором и третьем месте – образование и коммунальные услуги. Затем идут госорганы и силовые структуры.

Любопытно, что хакеры не считают достойным доверия такие формы всенародного голосования как электронное и почтовое голосование.

Подавляющее большинство респондентов (78%) заявили, что программных решений кибербезопасности с использованием искусственного интеллекта в ближайшие годы будет недостаточно для надежной информационной защиты. Полноценной замены человеческой способности анализировать пока не найдено.

Легальные, добропорядочные хакеры на службе у бизнеса и государства, работающие на платформе Bugcrowd, сумели в 2019 году предотвратить утечки информации, ущерб от которых составил бы 8.9 миллиардов долларов. За что и заработали (на законных основаниях!) на 38% больше, чем в предыдущем (2018) году. В следующий пятилетний период предотвращенный ущерб, по некоторым оценкам, достигнет 55 миллиардов.

Карьерные хакеры сегодня легально работают более чем в ста странах мира. Уровень их образования и квалификации достаточно высок. В Индии, например, Indian Institute of Science и ряд других вузов выпускают специалистов, пользующихся высоким спросом на мировом рынке труда. Индия вообще лидирует по числу профессионалов в области кибербезопасности наряду с США, Австралией и Великобританией, пишет А. Гупта.

Хакеров отличают такие качества и компетенции как прекрасная память, умение концентрироваться, критически, нелинейно мыслить, решать сложные

профессиональные головоломки, владеть разными языками.

Большинству опрошенных хакеров (53%) не исполнилось 24 лет. Более 60% из них мотивированы стремлением к самореализации, успешной карьере, благосостоянию.

Вместе с тем, авторы исследования отмечают возросшую социальную ответственность респондентов. 93% из них заявили, что полностью разделяют цели и миссию организации, в которой работают.

Отвечая на вопрос, каким путем они овладели знаниями и практическими навыками, большинство указало на онлайновые ресурсы, 30% процентов назвали себя самоучками, только 13% упомянули академическое образование или спецкурсы по кибербезопасности.

Как бы то ни было, пишет Гупта, 70% карьерных хакеров зарекомендовали себя наилучшим образом в тестировании безопасности веб-приложений.

Главный вывод исследования: несмотря на бум развития технологий искусственного интеллекта, человеческая смекалка и креативность остаются наиболее эффективным инструментом современной кибербезопасности.

# Рецензия

**Red Team: How to Succeed by Thinking Like the Enemy**
By Micah Zenko. 336 pages; $30.

Монография представляет собой развернутую характеристику основных принципов, функций и видов действий т.н. «красной команды», играющей роль противника в ходе сценарного анализа или «штабных игр», которые сегодня широко используются компаниями для изучения потенциальных угроз и рисков. На этих учениях исследуются и отрабатываются «лучшие практики» предупреждения и минимизации рисков.

Повествование ведется от имени профессионалов, выступающих за «красную команду», и иллюстрируется примерами, как почерпнутыми из реальной практики, так и придуманными, которые многие читатели вполне могут примерить к своим компаниям в разных отраслях.

Автор подробно характеризует три основных приема из арсенала «красной команды»: симуляция активности конкурента; тестирование уязвимостей в охранных системах компании; альтернативный анализ возможных ситуаций.

Книга охватывает широкий спектр применения концепции и методологии «красной машины»:

- армейские штабные игры;

- «красная команда» в сценарном анализе разведки и других государственных спецслужб;

- частный бизнес;

- футурология.

Книга не только информирует об истории, назначении, методологии и результатах реализации концепции «красной команды». Она предоставляет блестящий анализ новейших векторов и методов использования этого инструмента.

Монография, по мнению экспертов, чрезвычайно информативна и полезна широкому кругу специалистов по тестированию периметра и отдельных систем корпоративной безопасности, тренерам, организующим «штабные игры», профессиональным аналитикам в любой сфере бизнеса. Она достойна того, чтобы с ней ознакомились профессионалы, занятые в охранной индустрии.