АПКБ

АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

БЕЗОПАСНОСТЬ БИЗНЕСА В УСЛОВИЯХ ПАНДЕМИИ

Подготовлено Ассоциацией Профессионалов Корпоративной Безопасности Украины

Дорогие друзья!

Мир, Украина, бизнес и каждый из нас сейчас находится в очень непростой ситуации, с которой ранее не сталкивался.

Мы приняли решение, что подготовим рекомендации от каждого Комитета Ассоциации в едином документе и предложим его всем Вам.
Информации очень много и не так-то просто найти ту, которая соответствует действительности, поэтому особенно важно ориентироваться на мнение Профессионалов.

Будьте здоровы.
Председатель Правления АПКБУ
Сергей Погребной

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

СОДЕРЖАНИЕ

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

1. ОРГАНИЗАЦИЯ РАБОТЫ ПЕРСОНАЛА

1.1. Рекомендации Комитета Киберустойчивости Бизнеса

Наша цель – обеспечение непрерывности функционирования бизнеса и сохранение конфиденциальной информации в условиях неотвратимых кибератак.
Мы стремимся достичь этой цели путём создания инструментов, методологии и нормативной базы для обеспечения способности бизнеса:
- выявить и устранить уязвимости информационных систем;
- эффективно противодействовать кибератакам, управлять соответствующими рисками;
- оперативно реагировать на киберинциденты и кибератаки, быстро восстанавливаться после них.

01 Уделите достаточно внимания работе ключевых людей в компании, особенно тех, кто имеет доступ к финансовым операциям и критическим данным. Вплоть до того, что отправьте к ним домой системного администратора для проверки настроек сети, домашних устройств, корпоративного VPN.

02 Пересмотрите существующие доступы сотрудников к данным и сервисам, запретите все, что не является «первой необходимостью», и предоставляйте доступ только в случае аргументированного запроса, например:
- проведите инвентаризацию информационных систем (ИС), с которыми работают сотрудники;
- для каждой ИС получите список пользователей и их прав доступа;
- оцените, каким пользователям и к каким системам нужен постоянный доступ, а к каким лучше открывать по мере необходимости (например, для подачи отчётности раз в неделю/месяц).

03 Проведите работу с сотрудниками по части безопасности их удалённого рабочего места. Многие привыкли к свободному режиму использования программного обеспечения и онлайн-сервисов из дома. Теперь же там находится периметр вашей компании, поэтому правила нужно временно изменить, например:
- создать на личном устройстве отдельную учётную запись с минимально необходимыми правами (не администратора),
- для этой учётной записи установить минимальный набор программ, необходимых для работы (все должны быть лицензионными и регулярно обновляться);
- не использовать личные "облачные" сервисы (Google Cloud, Dropbox и т.п.) для передачи важной информации, только корпоративные "облака" и мессенджеры.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

04 Обратитесь к экспертам, которые помогут вам советом и опытом при таких изменениях в работе. На сегодняшний день есть большая потребность в:
- Помощи с переводом бизнес-процессов в режим удалённого офиса;
- Быстрой оценке рисков во время перевода и после него, а также управлении ними на данный момент и в долгосрочной перспективе.

05 Проводите сотрудникам тренинги по личной кибергигиене. Объясните на примерах - для чего использовать сложные пароли, двухфакторную аутентификацию (одноразовые временные пароли), обновлять программы, использовать защищённые коммуникации (безопасно обмениваться секретной информацией), делать резервные копии и т.д.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

1.2 Рекомендация Комитета Технических Средств Безопасности и Защиты Информации

Главным направлением деятельности Комитета является популяризация методов предотвращения рисков либо их минимизация с использованием технических средств.
Основными сферами применения технических решений являются:
- Защита материальных ценностей от посягательств с помощью сигнализации, видеонаблюдения, систем контроля доступа.
- Защита речевой информации от утечек и выявление следящей аппаратуры.
- Противодействие промышленному шпионажу.
- Выполнение задач контроля производственных процессов и их аналитика.
- Кибергигиена при использовании гаджетов.
- Решение нестандартных задач с применением специального электронного оборудования.
- Сфера применения техники для обеспечения безопасности бизнеса не ограничена и покрывает практически все запросы корпоративного сектора.

Безопасность периметра

01 Исключить возможность проникновения на территорию подконтрольных объектов (офис, производство, склад, ТРЦ и т.д.) людей, имеющих повышенную температуру путем использования инфракрасных бесконтактных градусников (пирометров) и/или в случае прохода большого количества людей, путём использования тепловизионных камер, с возможностью анализа температуры в потоке и одновременным контролем не менее 5 людей, с привязкой к фотофиксации и распознаванию лица из имеющейся базы.

02 Исключить или снизить до минимума использование контактных систем контроля и управления доступом, путём замены их на бесконтактные (по распознаванию лиц или венозных рисунков, без касания). В случае использования современных магнитных карт, запретить персоналу их физическое прикладывание к контролёру (стандартная дальность считывания до 5 см.) для уменьшения контакта с потенциально зараженной поверхностью. На время карантинных мероприятий СКУД, построенный на базе систем биометрии (с непосредственным прикладыванием пальцев или глаза) дополнить магнитными бесконтактными считывателями, в случае если это возможно.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

03 Перейти на использование мобильных идентификаторов в системах контроля доступом. Это позволит свести к «0» физический контакт между людьми, связанных с администрированием выдачи пропусков (карт), а также предоставит возможность системам контроля доступа производить идентификацию сотрудников на расстоянии до 10 метров.

04 В случае использования систем OSINT* при заражении либо подозрении на заражение одного из сотрудников, используя системы «геолокации» (Bler, COVID19), видеонаблюдения и контроля доступа в офисе и на объектах, определить потенциальный круг контактов и сократить их пребывание на рабочих местах (максимальная изоляция).

Переход на удаленную работу

01 Определить сведения, которые нужно контролировать, для обеспечения информационной и технической безопасности. Закрепить регламентирующим документом «Перечень информации, составляющей коммерческую, финансовую тайну и иные». В дополнение к перечню информации, составляющей тайну, создать регламенты, регулирующие информационную безопасность, если их не было ранее.

02 Установить круг лиц, которые имеют допуск к финансовым или иным конфиденциальным сведениям. Определить, кому из сотрудников компании для работы нужны эти данные. Выделить тех, кому требуется постоянный допуск, для остальных работников прописать порядок подачи запросов на предоставление информации.

03 В приказном порядке, определить круг сотрудников, имеющих корпоративную технику и определённые уровни доступов, и запретить им перемещение по городу на общественном транспорте, в т.ч. такси. В случае отсутствия собственного транспорта – выделить корпоративный.

04 Довести до сведения рядовых сотрудников, работающих на «удаленке»*, информацию о том, что использование личных средств мобильной связи (вместо заранее настроенных и подготовленных ноутбуков или корпоративных средств связи), для проведения конференц-звонков, а также проведения совещаний из мест, для этого не предназначенных – подразумевает соблюдение определённого «телефонного этикета» и использования так называемого «птичьего языка»*, для донесения информации до собеседника, во избежание утечки конфиденциальной информации.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

05 Довести до сведения сотрудников ТОП уровня, о возможности удалённого аудио- и видеоконтроля помещений (в т.ч. личного кабинета), путем установки средств НСИ (несанкционированного съёма информации) или использования направленных микрофонов. С целью недопущения утечек конфиденциальной информации, провести (регулярно проводить) проверку помещений (в т.ч. автомобилей, яхт и т.д.) из которых осуществляется управление предприятием(-ями), с последующей обязательной дезинфекцией проверенного помещения. Разработать инструкции о противодействии и недопущении перехвата информации в «домашних» условиях и довести их до персонала под роспись.

06 Довести до сведения всех сотрудников, о возможности использования против них мошеннических систем «deepfake» - методика синтеза изображения, основанная на искусственном интеллекте (аналог – «Джокер», использование клона мобильных телефонных карт), с целью создания видео/аудио роликов с лицами и/или голосами собственников и передачи ложной команды на выполнение тех или иных действий противоправного характера. С целью недопущения реализации данной схемы, разработать и утвердить на уровне руководства СБ контрольные вопросы или знаки, которые позволят визуализировать и «офизичить»* лицо, с которым происходит беседа.

07 Для возможности физического контроля удалённой работы в случае необходимости использовать платформу для централизованного управления инфраструктурой ключей (сертификатов). Использование данной платформы позволяет исключить ряд угроз для информационной безопасности организации, будь то локальный доступ к информации или удалённый, путём использования комплекса решений по строгой аутентификации и шифровании транзакций между рабочими станциями сотрудников или для связи с центральным сервером. Данная платформа использует уникальную запатентованную технологию аппаратного шифрования канала обмена данными между сервером и чипом смарт-карты, что обеспечивает максимальный уровень безопасности при выдаче и управлении сертификатами, OTP-ключами* и др., а также исключает хранение сотрудниками паролей в открытом виде. Использование такого рода зашифрованного соединения исключает любую возможность перехвата или подмены сертификатов, OTP-ключей, цифровых подписей и пр. злоумышленниками.

08 Для работы с конфиденциальными документами (в том числе финансовыми, клиент-банком, и т.д.) высокого уровня значимости, использовать специальное антихакерское оборудование (защищённые ноутбуки), с минимальной возможностью перехвата данных и инфицированием системы.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

09 Использовать закрытые корпоративные мессенджеры без возможности извлечения переписки, но с допустимостью использования собственной клавиатуры мессенджера (для исключения «логирования»), с возможностью мгновенного удаления переписки без восстановления на вашем устройстве, даже имея пароль и логин доступа.

10 Довести до сведения сотрудников о появлении большого количества ложных (фейковых) мошеннических сервисов, которые могут быть замаскированы под платформы для проведения конференций, онлайн обучения, сервисов по доставке еды, аптек, товаров первой необходимости и т.д. В том числе, довести информацию о появлении (появилось) большого количества «фейковых» информационных сайтов, о COVID-19 и волонтёрских организациях, собирающих деньги на помощь в борьбе с вирусом. В связи с этим, на уровне приказа по предприятию, запретить использование сторонних (несогласованных) сервисов для проведения переговоров и презентаций и в рекомендательном порядке (в случае использования корпоративной техники, приказном) запретить использования любых сервисов с пересылкой форм с личными и/или корпоративными данными, в т.ч. любой платежной информации, до согласования с администратором сети, департаментом ИТ и ИТ безопасности или представителями СБ предприятия.

11 Вне зависимости от принадлежности техники (корпоративная или личная) определить необходимый минимум приложений, обеспечивающих достаточный уровень безопасности содержимого. В зависимости от обстоятельств, стоит рассмотреть подключения к терминальным серверам без права копирования информации.

12 Вся передаваемая информация на носителях должна быть зашифрована корпоративным ключом с использованием как программных, так и аппаратных средств шифрования. В случае невозможности использовать сторонние продукты, рекомендуется полнодисковое шифрование.
В случае, если корпоративные правила допускают, возможно, использование DLP* систем - систем оперативного перехвата и анализа информации с компьютера сотрудника (контроль за ключевыми словами, почтовыми адресами, перехват разговоров в скайпе, перехват входящих и исходящих файлов и сообщений и т.д.), с целью предотвращения утечки конфиденциальной информации. В том числе, данные системы позволят проконтролировать реальное время, проведенное сотрудником за компьютером (СКУД). О данной возможности сотрудник может оповещён, либо возможно использование скрытого агента.

13 В обязательном порядке использовать VPN* для подключения сотрудников к корпоративной сети.

14 Использовать многофакторную аутентификацию (MFA), которая предоставляет доступ к облачным ресурсам и другим системам только для авторизованных пользователей, без возможности использования каналов передачи данных в открытом, незашифрованном виде (например, СМС).

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

Глоссарий

OSINT – open source intelligence – разведка из открытых источников (сбор данных).

Птичий язык — так называемый стиль речи, который использует, перегруженную терминами и затемняющую смысл формулировками, понятную только немногим людям, участвующим в беседе.

«Удаленка» – работа сотрудников вне офиса.

«Офизичить» – профессиональный сленг, подразумевающий деанонимизацию (сопоставление нескольких аккаунтов одного человека) субъекта или персоны.

OTP-ключ - one time password – одноразовый пароль — пароль, действительный только для одного сеанса аутентификации. Действие одноразового пароля также может быть ограничено определённым промежутком времени.

DLP-система - Под DLP-системами принято понимать программные продукты, защищающие организации от утечек конфиденциальной информации. Сама аббревиатура DLP расшифровывается как Data Leak Prevention, то есть, предотвращение утечек данных.

VPN (Virtual Private Network «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

1.3 Рекомендации Комитета Охраны Труда

Основными задачами Комитета является информирование, обучение и консультирование членов АПКБУ в вопросах, связанных с системами управления безопасностью производственных процессов, и, как следствие, снижение потерь, связанных с авариями, происшествиями и травмированием персонала на основе лучших мировых практик. В рамках выполнения данной задачи планируется проведение открытых заседаний комитета, организация обучающих конференций и семинаров по различным направлениям, таким как: оценка рисков, определение коренных причин происшествия, оказание первой доврачебной помощи, транспортная безопасность и т.д.

01 Берегите своё время. Разработать процедуру, презентацию, оценку рисков, чек-лист для противодействия COVID-19. Есть вероятность, что кто-то уже разработал это до Вас и распространил, и для этого мы создали специальный ресурс **esosh.net/protydiya-covid-19/**, где выкладываем материалы, разработанные коллегами из различных предприятий. Распространяйте, пожалуйста, свои наработки, а для размещения на ресурсе «Esosh» присылайте информацию на нашу почту: office@esosh.net.

02 Диджитализация. Самое время реализовать инструктажи, обучение по охране труда и проверку знаний онлайн и дистанционно – с помощью видео, презентаций, тестов. Особенно ценно, если сможете оцифровать информацию о состоянии здоровья, а также медицинские карты работников.

03 Обеспечение средствами индивидуальной защиты СИЗ - это не только маски или респираторы, но и защитные очки и перчатки - стандартная защита для людей с высокой группы риска. К ним относятся лица, работающие с большим количеством людей или мест (охранники, медперсонал, работники столовой, уборщицы, супервайзеры, кладовщики и т.п.) – и именно на них рассчитан ресурс СИЗ предприятий. Не потому что их жалко раздать каждому работнику, а по причине того, что сейчас по всему миру их не производится в достаточном количестве. Большинство работников относятся к этому с пониманием, но есть и те, кто и не пренебрегает при первой возможности забрать маски/ респираторы/ дезинфицирующие средства домой или на продажу. Обязательно объясняйте в коллективах, что недостаток СИЗ может привести к остановке предприятия и потере работы в такое трудное время, как сейчас.

04 Утилизация СИЗ – также под контроль. Сдал старый респиратор (герметически упакованный в полиэтиленовый пакет) в специальный контейнер, получил новый – это является ещё одним методом контроля оборота СИЗ.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

5. Выявление больного либо с подозрением на COVID-19:

5.1 Изолировать сотрудника с подозрением в отдельное помещение, выдать защитную маску.

5.2 Проинформировать учреждение по охране здоровья о подозрении у сотрудника заболевания с целью организации его проверки при помощи тест-систем либо лабораторных обследований на коронавирус.

5.3 Определить список контактов за последнюю неделю (минимум), как на работе, так и дома:
- составить поименной список контактной группы и мест пребывания особы;
- передать список представителям органов контроля (медицинских заведений, санэпидемстанции, районные администрации);
- проинформировать контактную группу сотрудников о подозрении на возможное инфицирование;
- сотрудников (присутствующих на рабочих местах) контактной группы отправить на самоизоляцию с постоянным/систематическим мониторингом их состояния здоровья;
- осуществить инструктаж сотрудников из числа контактной группы, о порядке действий в случае выявления у себя или членов семьи симптомов коронавируса;
- самоизоляцию контактной группы осуществляется до момента определения точного диагноза подозреваемого на коронавирус (подтверждения или опровержения факта инфицирования);
- провести дезинфекцию всех мест пребывания сотрудника с подозрением на коронавирус с подключением специализированной организации.

5.4 Самостоятельно не меряем температуру, не контактируем, не делаем санитарную обработку помещений.

06 Столовые - закрывать или ограничить? Решение: расстояние в очереди 1.5 м, только буфет и упакованная еда, раздельные перегородки из оргстекла на столах между теми, кто принимает пищу, усиленный режим вентиляции.

07 Бесконтактные термометры – из-за холодного воздуха на входе в помещение обычно показывается температура, намного ниже реальной. Поэтому организовывайте замеры подальше от мест перепадов температур.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

2. ПРОТИВОДЕЙСТВИЕ ПОСЯГАТЕЛЬСТВАМ НА ИМУЩЕСТВО КОМПАНИИ

2.1. Рекомендации Комитета Руководителей Служб Безопасности

Комитет Руководителей Служб Безопасности создан с целью выполнения уставных задач Ассоциации. Среди основных задач деятельности Комитета можно выделить следующие:
- Формирование корпоративного Реестра руководителей служб безопасности компаний, предприятий, учреждений и организаций в Украине.
- Установка и настройка сети профессионального партнёрства и сотрудничества между руководителями служб безопасности.
- Содействие развитию профессионального рынка услуг по направлению «Менеджмент корпоративной безопасности предприятия».
- Разработка и популяризация стандартизированного подхода к профессиональным требованиям для должности «Руководитель Службы Безопасности Предприятия».
- Сотрудничество с другими Комитетами АПКБУ по вопросам поддержания условий для развития предпринимательства в Украине, наработки и реализации механизмов защиты бизнеса – как путём совершенствования законодательства, так и развития рынка корпоративной безопасности.
– Взаимодействие с представителями правоохранительных органов и контролирующих инстанций по вопросам содействия снижению общего уровня преступности в Украине, путём укрепления рынка корпоративной безопасности.
- Подготовка материалов для разработки нормативно-правовой базы по продвижению законодательной инициативы в форме Закона Украины «Про Корпоративную Службу Безопасности» и других законов и подзаконов нормативно-правовых актов в сфере корпоративной безопасности.

Основными направлениями и приоритетами деятельности Комитета являются:
- Организация и проведение для членов АПКБУ семинаров и рабочих встреч по вопросам управления корпоративной безопасностью на предприятиях;
- Обмен опытом и лучшими практиками, а также предоставление необходимой помощи членам АПКБУ в решении вопросов, связанных с недостатками систем управления безопасностью на предприятиях;
– Участие в работе совещательных органов (межведомственных комиссий), общественных советов и т.д.) при профильных центральных органах власти;
- Другая смежная деятельность, которая соответствует уставным требованиям АПКБУ и имеет целью популяризацию и совершенствование стандартов системы управления корпоративной безопасностью предприятий.

В связи з распространением эпидемии коронавируса COVID-19 и введением масштабных карантинных ограничений, происходят кардинальные изменения условий ведения бизнеса как в Украине, так и во всем мире. Экономические и социальные изменения, которые будут происходить в ближайшее время, приведут к значительному переформатированию традиционного ландшафта рисков и угроз беспрерывности ведения бизнеса.

В ответ на новые вызовы, Комитет СБ АПКБУ разработал перечень рекомендованных мер на период вирусной пандемии, чтобы помочь обеспечить безопасность ЛЮДЕЙ – главного стратегического ресурса каждой организации.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

I. Общие рекомендации для бизнеса

В период значительного риска для здоровья людей и угрозы ведения бизнеса, компания должна проводить все необходимые от неё меры для обеспечения личной безопасности персонала и устойчивости компании при угрозе заражения, а именно:

01 Осуществлять каждодневный онлайн мониторинг состояния здоровья сотрудников.

02 Проводить анкетирование сотрудников с целью выявления признаков и потенциальных угроз заражения.

03 Подготовить т.н. «Карты возможного заражения» среди сотрудников компании, которые:
- Осуществляли поездки в период январь-март 2020 годы за границу, в частности в страны с высоким порогом инфицированных;
- Имели контакты с особами, которые установлены по медицинским заключениям как носители коронавируса;
- Имеют явные симптомы заболевания вирусом как у себя, так и у членов семьи или ближайших родственников.

04 Допуск на рабочее место осуществлять только при условии индивидуального измерения температуры тела, или с использованием групповых термальных датчиков.

05 Обеспечить сотрудников офисного помещения средствами индивидуальной защиты:
- антисептиками;
- масками и респираторами (рекомендуемые - 3М, класс ff2 и ff3);
- нитриловыми перчатками (по несколько пар в смену);
- лабораторными накидками и спецодеждой 3-4 класса защиты по стандарту ANSI / AAMI PB70 2012.

06 Обеспечить доставку сотрудников, работающих на постоянной основе, к месту работы / офиса.

07 Организовать антивирусную обработку служебного автотранспорта.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

II. На что обратить внимание руководителю СБ?

01 В то время, как большая часть сотрудников находится дома и вынуждена работать в удаленном режиме, в первую очередь нужно придерживаться уже организованного режима санитарной гигиены для сотрудников, которые вынуждено остались в офисе, на территории либо в помещении предприятия (например, охрана и т.д.). Поскольку предприятия находятся на карантине, в офисах и в других помещениях, как правило, круглосуточно отсутствуют сотрудники. Поэтому рекомендуется сосредоточиться на охране именно таких объектов, а также зон критической инфраструктуры.

02 При наличии системы видеонаблюдения, следует обеспечить установку бесперебойного и резервного источника питания, с целью организации контроля за мониторами и архивированием видеозаписей. В случае отсутствия сигнализации указанных помещений, следует принять максимально возможные меры к её немедленному установки.

03 При наличии на объекте физической охраны, провести ревизию и выявить «узкие места», которые образовались, а также обновить задачу для охранников по защите объекта, его освещённости, защищённости, экипировке и обеспечению охранников СИЗ;

04 Продумайте логистику доставки сотрудников охраны при условии ограничения передвижений в общественном транспорте, а также предусмотрите альтернативный вариант их доставки. Все это нужно, поскольку в условиях, возникший криминалитет быстро переквалифицируется с «домушников» и, очевидно, будет осуществлять кражи в отношении объектов, которые будут оставаться без присмотра. В первую очередь это касается отдельно стоящих офисных помещений, складов и т.д.

05 Поскольку сотрудники работают в удалённом режиме, подразделениям информационных Систем компании необходимо разработать отдельные рекомендации по работе в домашних условиях, с целью обеспечения конфиденциальности информации, начиная с использования паролей, недопущения работы на оборудовании других членов семьи и т.д. и предотвращения утечки служебной и иной критической информации. Создать и запустить отдельные мессенджеры для соответствующих служебных групп с целью обмена информацией и поддержания связи. Также следует провести инструктаж работников о формах связи с руководством и коллегами по работе, посредством использования телефонной связи, общения в текстовом формате в рекомендованных мессенджерах, для того, чтобы исключить возможное снятие конфиденциальной информации с незащищённых каналов связи и открытых источниках.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

06 Позаботиться о психологической поддержке сотрудников со стороны их непосредственных руководителей, в т.ч. ежедневный контакт по тем каналам связи, которые были согласованы ранее, при условии соблюдения режима карантина, установленного соответствующими ограничениями.

07 Устанавливать работникам в ежедневном режиме операционные задачи и требовать отчёт об их выполнении. Тем самым обеспечить фокус сотрудников на выполнении задач, а не на получении негативной информации с медиа и СМИ об активизации распространения пандемии и ее негативном влиянии.

08 Не стоит ожидать ослабления активностей и со стороны правоохранительных органов. Напротив, они могут вести себя ещё более жёстко и коррумпировано, с целью возможного быстрого получения неправомерной выгоды или содействия рейдерским захватам. В связи с этим, необходимо провести ревизию документооборота в офисе на наличие не утилизируемых документов, записей, техники и т.д., а также конфиденциальной информации, которая может на них содержаться.

09 Также следует пересмотреть подход к организации технических систем безопасности предприятия, путём внедрения дополнительных мер контроля СКД и других имеющихся систем.

10 Следует ежедневно отслеживать открытые реестры собственности недвижимого имущества, судебных решений и т.д., с целью возможного установления информации по фактам изменений данных, которые могут повлиять на вероятность незаконного отчуждения имущества или проведения обысков, других процессуальных действий.

11 Стоит свести к минимуму оборот наличных средств, если это имело место быть. Организовать контроль за целесообразностью проведения всех транзакций онлайн и с использованием терминалов.

12 Сформировать совместно с ТОП менеджментом и линейными руководителями карту рисков компании, связанных с COVID-19 - стратегических и операционных. Провести оценку их влияния на процессы и возможность управления рисками, в первую очередь по их минимизации. Закрепить каждый риск за руководителями или ответственными лицами для быстрого реагирования на индикаторы их изменения. Исходя из созданной карты рисков, связанных с COVID-19, согласовать План неотложных мероприятий, направленных на обеспечение непрерывности и функционирования компании в режиме чрезвычайной ситуации.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

III. Базовые потенциальные риски, которые будут характерны для бизнеса

01 Значительный финансово-экономический спад в развитии предприятий, аж до закрытия некритических направлений бизнеса.

02 Внесение изменений в стратегию функционирования предприятия, з учетом обстоятельств, которые имеют место быть.

03 Изменение ценовой политики компании на работы, сервисы и услуги.

04 Несвоевременное реагирование со стороны бизнеса на законодательные изменения, которые принимаются в ответ на распространение пандемии.

05 Кредитные риски по причине изменений условий кредитования со стороны банков.

06 Сбой в сети поставок (на любой цепочке).

07 Отказ перевозчиков и транспортных компаний в предоставлении услуг по причине введенных ограничений.

08 Очевидная активизация фактов недобросовестной конкуренции.

09 Потеря или существенная корректировка клиентской базы и базы поставщиков, которые не справились с возникающими вызовами.

10 Факты краж и потери имущества и собственности (в т.ч. интеллектуальной) из-за ослабления мер охраны и форм контроля.

11 Необходимость пересмотра договорных и трудовых отношений с персоналом и контрагентами.

12 Психологическое напряжение, связанное с поддержанием бизнеса как со стороны акционеров, так и менеджмента и сотрудников, которые переведены на дистанционную форму работы.

13 Низкая мотивация и отсутствие действенного контроля за работниками, которые перешли на удалённый режим работы.

14 Ослабленное обеспечение системы документооборота и администрирования бизнеса, который потерпел изменения.

15 Другие совокупные риски.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

Выводы

Имеющийся кризис – это возможность самопроверки зрелости выстроенных систем безопасности компании. Сейчас наочно видно эффективность работы служб, ответственных за корпоративную культуру и риск-менеджмент, профессионализм IT сотрудников и всех критических функций, и, в первую очередь, подразденлений безопасности. Атмосфера эффективности не строится за один день, а сегодняшний кризис – это экзамен как самой системы, так и каждого из нас на предмет стойкости, гибкости и способности справляться с сегодняшними неожиданными вызовами.

Победа над угрозой и минимизация влияния на бизнес возможна только при условии привлечения всего коллектива, всех подразделений к эффективной работе по реализации Плана мероприятий, направленного на обеспечение непрерывности и функционирования компании в режиме чрезвычайной ситуации, использование правильной информации, осознание всех видов угроз и активного использования такого инструмента, как риск-менеджмент.

Важно помнить, что в случае невозможности самостоятельно справиться с непростыми вызовами на уровне отдельно взятой компании, эксперты АПКБУ и представители партнерских сервисных компаний по направлению безопасности всегда готовы Вам помочь.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

2.2. Рекомендации Комитета Частной Детективной и Охранной Деятельности

Основной целью комитета является разработка и внедрение стандартов в сфере частной охранной и детективной деятельности.
Основные направления деятельности – сохранение и защита материальных активов, противодействие неправомерным посягательствам со стороны злоумышленников, защита персонала, проведение расследований, а также участие в разработке профильных законопроектов.

01 Пересмотреть состав дежурных смен. Составить список критических постов и определить минимально необходимое количество людей (посты, которые существенно влияют на общую защищенность объекта (объектов) компании, пропускной режим, защита от внешних угроз). Менее критические - временно закрыть, персонал перевести на другие посты или использовать как резерв.

02 Обеспечить личный состав дежурных смен всеми необходимыми средствами защиты (с запасом). Организовать уборку помещений постов (КПП) и их дезинфекцию.

03 На инструктаже дежурной смены – обязательно ежедневно проводить температурный скрининг. Заболевших немедленно изолировать и отправлять домой под наблюдение врачей. Инструктаж проводить исключительно в медицинских масках.

04 Дежурная смена несет службу в защитных масках, обрабатывает руки дезинфицирующими средствами.

05 При уменьшении количества персонала (заболевшие либо те, кто имеют трудности с прибытием на роботу и т.д.) оптимизировать количество постов и состав дежурной смены. Доставка персонала, который проживает за пределами города – сформировать экипажи и приезжать на работу на личных машинах.

06 При наличии неблагоприятных условий – перейти на вахтовый метод несения службы (составить две смены минимально необходимого персонала. Одна смена – на дежурстве, другая – отдыхает). При этом необходимо заблаговременно создать соответствующие бытовые условия (комната отдыха, кровати (раскладушки), одеяла, смена белья, трехразовое питание, душевая и т.д).

07 Максимально использовать технические средства защиты и охраны.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

08 Свести до минимума количество посетителей, клиентов, работников подрядных организаций, а при входе на объект (территорию) обязательно проводить их температурный скрининг. В случае выявления заболевших – доступ на территорию (в офис) – категорически запретить, действовать по протоколу.

09 В критических ситуациях полностью запретить доступ посетителей. Разрешить только тем, чья работа влияет на поддержание жизнедеятельности объекта (водо-, газо-, электрообеспечение и т.д.).

10 По возможности организовать «сквозной поток посетителей» (вход – через один пост охраны, выход – через другой), тем самым не будет скоплений людей на проходных (КПП).

11 Особое внимание обратить на водителей транспортных средств.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

2.3. Рекомендации Комитета Форензик

Комитет Форензик создан с целью обмена бесценным опытом между передовыми специалистами рынка в части расследования кейсов корпоративного мошенничества в компаниях и определения методов противодействия таким недобросовестным действтям!

01

Во время кризиса, особое внимание нужно уделять кибергигиене. Почему?
Потому что в условиях пандемии бизнес перешел в режим удаленной работы, а это означает -максимально «диджитализировался».
Основные риски:
- Незаконный перехват ключей от клиент-банка у бухгалтера.
- Массовая рассылка фишинговых писем с целью получения данных о «логах» корпоративного почтового ящика.
- Преднамеренное заражение компьютера вредоносным ПО с целью выкачки конфиденциальных данных компании: ее управленческого учёта, клиентс кой базы и прочего.
Решение: провести он-лайн тренинг для сотрудников компании с целью информирования о потенциальных рисках.

02

В условиях удалённой работы, когда предприятия работают в режиме гибернации, особое внимание стоит уделять сохранности активов и запасов компании. Согласно Мировой и украинской статистике, незаконное отчуждение Активов даже не в период пандемии - это риск #1 для компании.
Решение: усиление физической безопасности, расстановка камер по периметру предприятия с учётом материальности нахождения активов и слепых зон камер. Установка усиленного контрольно-пропускного режима и охрана предприятия по его периметру.

03

Усилить финансовый контроль компании, контроль главного бухгалтера в части осуществления любых платежей, направленных на закупку чего-либо. Минимизация и контроль Ф2 на предприятиях. Риск кражи наличности. Контроль списания основных средств не по рыночной цене с целью их реализации.

04

Чёткий контроль дебиторской задолженности в разрезе контрагентов со стороны службы экономической безопасности. Есть риски манипуляции в части кредитования контрагентов за счёт терменирования ее погашения, также списание деберской заложенность и запасов компании.

05

Карантин - это отличная возможность описать бизнес процессы компании и положить их в основу баковых политик компании (политики закупок и продаж, политики списания и учёта, мотивационной политики менеджеров по продажам и регламентов тендерного комитета и т.д.), риск матрицы и системы комплаенс, у кого нет. Карантин позволяет усилить систему внутренних контролей в спокойном режиме. Собственникам и начальникам службы безопасности на заметку.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

2.4. Рекомендации Комитета Полиграфологов

Основным направлением нашего Комитета является популяризация методики проверок на полиграфе – профессионального подхода, помощника и партнёра для Собственников, СБ, ТОП-руководителей компаний. Для этих целей планируется организовывать и проводить онлайн-мероприятия, круглые столы, обсуждения, статьи и другие формы продвижения. Как только карантин завершится и проведение мероприятий станет безопасным, Комитет планирует провести семинар "Полиграф на службе безопасности Бизнеса".
Важной составляющей нашей работы является проведение разъяснительной работы среди компаний – развеивание мифов, опровержение слухов о методике проверок на полиграфе, представление кейсов из практики и подходов для представления эффективности и полезности методики.

01

Тихая украинская ночь, но сало надо перепрятать
Все, кто ранее не успел либо не смог поставить в офисах видеонаблюдение, сейфы, укрепить входы и замки, у кого пароли от сейфов знают практически все сотрудники - самое время усилить охрану, переместить все ценные вещи в другие более защищённые места, поменять пароли и ключи. Любым способом создать как можно больше проблем и барьеров для потенциальных злоумышленников, чтобы они не смогли воспользоваться отсутствием охраны либо контроля. Как показывает практика, в 70% случаев ограблений и краж в офисах, криминал практически всегда действует сообща с сотрудниками бизнеса, как действующими, так и недавно уволившимися, которые знают все систему охраны и сигнализации изнутри.

02

Удалённая работа – спасение бизнеса или высокий риск слива КИ
Как было упомянуто выше, многие компании были вынуждены перейти на удалённый режим работы в связи с карантином. Для защиты здоровья своих сотрудников — это несомненно верное и действенное решение. НО! Одновременно с этим карантин несёт опасность для бизнеса, по причине того, что РИСКИ СЛИВА КИ (конфиденциальной информации) повышаются многократно.

У многих компаний до кризиса не было необходимости продумывать вопрос - как безопасно организовать этот процесс? Когда весь персонал работал в офисе и меры защиты применялись на стационарных компьютерах, вопрос защиты данных находится под контролем. НО, когда вы работаете в удалённом режиме на своем личном компьютере, где установлены различные программы, резко повышается не просто риск попадания вируса на вас девайс, но и «слив» рабочей информации. При этом, когда сотрудник работает удаленно, за ним по сути нет контроля. Поэтому в условиях «удаленки» важно организовать для каждого сотрудника рабочий компьютер, на котором будет установлен определённый перечень программ и инструкция с выполнением всех требований кибербезопасности.

Важно напомнить каждому сотруднику о требованиях подписанного договора о неразглашении КИ. Если же такие договора не были разработаны и подписаны ранее – рекомендуем незамедлительно заняться этим вопросом. Также не будет лишним озвучить всему вашему коллективу, когда закончится карантин. Возможны проверки на полиграфе тех лиц, к которым у компании возникнут вопросы.

03

Не принимайте на работу тех сотрудников, которые раньше наносили вред и/или воровали у компании

В первую очередь этот пункт относится к тем компаниям, которые продолжают работать и обеспечивать в условиях кризиса привычный режим жизни людей. Почты, банки, производство продуктов питания, аптеки, онлайн-доставка, продуктовые магазины и другие компании.

Если кризис будет продолжительным, будьте уверены - в эти компании начнёт выстраиваться очередь из желающих работать на любой должности, чтобы получить хоть какой-то источник дохода. При этом, у каждого человека есть свой «бэкграунд» – кто-то работает честно, а кто-то наживается на ситуации, ворует сам и/или вступает в сговор и совершает служебные хищения. Если Вы пропустите в свою компанию таких людей, риски и ущерб компании будут колоссальными. Оградите свой бизнес от рисковых людей, сохраните его для честных и порядочных сотрудников!

04

Примите сейчас такие сложные, но нужные кадровые решения

Одна из главных проблем для определённой категории собственников бизнеса – это нежелание принимать справедливые, но порой жёсткие решения в отношении сотрудников, к которым ранее были вопросы, подозрения в их благонадёжности и лояльности к компании.

Работа каждого сотрудника до начала кризиса должна быть обязательно проверена (особенно это касается тех, кто работает в компании более 5 лет и знает компанию, а ранее могли приносить ей пользу и прибыль). Осуществляем проверку на предмет:

- откатов и взяток,
- использования ресурсов бизнеса в корыстных целях,
- зеркального бизнеса и других рисков.

Собственник, узнав об этих фактах, может быть не готов, не иметь желания/смелости принять такое необходимое решение об увольнении недобросовестного сотрудника. Мотивы простые – «этот сотрудник работает давно, давайте дадим ему ещё один шанс, давайте повременим и не будем резать сгоряча» и многие другие отговорки.

Наша рекомендация - если у Вас в компании остались такие сотрудники, самое время принять решение об их увольнении. Иначе они «потопят» не только лично Вас, но и Ваш бизнес.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

3. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

3.1. Рекомендации Комитета Руководителей Юридических Служб

Цели и направления работы Комитета: объединение руководителей юридических служб компаний для формирования политик по работе с рисками и угрозами бизнеса, общих практик, направленных на защиту активов, построению эффективного взаимодействия юридических служб со службами безопасности в компаниях.

01 Работа юристов во время карантина очень важна для жизнеобеспечения бизнеса во время карантина. Для этого необходимо организовать непрерывное взаимодействие и коммуникацию с юридическими службами и согласование с ними всех управленческих решений, которые принимаются во время карантина.

02 Обеспечьте ежедневный мониторинг законодательства юридическими службами и рассылку аналитических справок всем подразделениям бизнеса для оперативного реагирования на изменения.

03 В связи с участившимися проверками предприятий СЭС совместно с Нацполицией на предмет соблюдения карантинных мер, приведите в порядок всю внутреннюю документацию и проконтролируйте соблюдение требуемых нормативными актами процедур (температурные замеры на входе, наличие персональных средств зашиты для сотрудников и т.д.) Также необходимо обеспечить дежурство в офисе как минимум одного юриста для сопровождения проверок на случай таких визитёров.

04 Приведите в порядок кадровые юридические дела. Если сотрудники работают дома на «удаленке», об этом должен быть вынесен соответствующий приказ по предприятию, подписанные заявления сотрудников с обязательством выполнять свои трудовые обязанности надлежащим образом.

05 Напомните сотрудникам о Политике и обязательствах о неразглашении конфиденциальной информации и сведений, составляющих коммерческую тайну. Если таких документов на предприятии нет, поторопитесь их внедрить.

06 Многие бизнеса в текущем статусе имеют проблемы с ликвидностью и дефицитом оборотных средств, среди таковых могут быть Ваши дебиторы. Некоторые уходят от обязательств путём банкротства и сворачивания бизнеса. Обеспечьте постоянный мониторинг их платёжеспособности по таким критериям, как судебные процессы, банкротство, изменение руководящего состава, акционеров/участников общества, изменение адреса, регистрации.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

3.2. Рекомендации Комитета Судебной и Криминально-Правовой Защиты

Главными направлениями деятельности Комитета являются популяризация законным методов и инструментов судебной и уголовно-правовой защиты, разработка законодательных изменений и подзаконных нормативных актов, просветительская деятельность и образовательные проекты, а также создание совместных продуктов с другими комитетами АПКБУ.

01 В случае, если у вас есть судебные споры, продолжайте качественного готовиться к ним, вовремя высылать все процессуальные документы, уточняйте информацию о проведении судебных заседаний. Карантин пройдёт, а вот судебные решения все равно придётся выносить. И каким они будут зависит сегодня от вас!

02 Внимательно следите за действиями своих дебиторов. Понимая, что рано или поздно долги придётся отдавать, многие, к сожалению, уже сейчас начинают уводить ликвидное имущество. Меры противодействия этому есть!

03 В смутные времена конфликты не рассасываются и не исчезают. В некоторых случаях они разгораются с новой силой. Уже сейчас возрастает количество рейдерских атак, исчезают регистрационные записи в реестре, уходят на третьих лиц корпоративные права. Сделайте аудит защищённости своих активов! Подключите смс-маяк! Подвергните строгой ревизии свой затянувшийся или начавшийся конфликт. Возможно именно сейчас пора действовать.

04 Не забывайте о том, что правоохранительная система продолжает работать! Следственные действия никто не отменял! Уголовные дела продолжают расследоваться! И да, Вы неожиданно можете получить повестку на допрос, определение суда о выемке документов или обыска в офисе. И к такой ситуации вы тоже должны быть готовы. Поддерживайте связь со своим адвокатом, оговорив потенциальные случаи неожиданных гостей, возможность его личного прибытия на следственное действие, наличие у адвоката средств защиты (маски, респиратора, перчатки, бахилы)! Подготовьте дежурных сотрудников в офисе и инструкции для них на случай внештатных ситуаций! Поддерживайте контакт со следователем!

05 Проведите ревизию всей документации в печатном виде! Вы должны быть чётко убеждены, что она хранится в правильном месте и правильным способом. Проверьте систему защиты вашей электронной информации и документации! Периодически инструктируйте сотрудников о правилах обращения с электронной информацией, электронной цифровой подписью и паролями!

4. ИНФОРМАЦИОННОЕ СОПРОВОЖДЕНИЕ

Рекомендации Комитета Антикризисных Коммуникаций

Комитет по вопросам антикризисных коммуникаций рассматривает коммуникационную активность компаний как способ обеспечения корпоративной безопасности и непрерывности ведения бизнеса.
Мы считаем, что работа с репутационными рисками должны быть поставлена на системную основу, поскольку это позволяет создать запас антикризисной устойчивости и сформировать «антихрупкую» репутацию.

«Коронавирусный» кризис, с которым сегодня столкнулся бизнес, беспрецедентен – это классический «чёрный лебедь», внезапный и беспощадный. Мир глобализирован и разделен одновременно, диджитализирован, и при этом в наиболее экономически активных странах находится в состоянии принудительного ограничения спроса и предложения на товары и услуги. Ломается весь привычный экономический уклад, который уже не может быть восстановлен в прежнем виде, а изменится пока ещё до конца не известным нам образом.
Соответственно, большинство case-stories антикризисного управления бесполезны в силу уникальности внешних условий работы компаний. Это время думать своей головой, а не искать готовые рецепты. Беспрецедентные исторические условия требуют соответствующих духу времени решений и людей, способных такие решения принимать.
Применительно к корпоративным коммуникациям сегодня целесообразно придерживаться следующих рекомендаций:

01 Добейтесь создания в компании дееспособного антикризисного штаба с участием PR-лидера. И постарайтесь быть в курсе реального положения дел в компании.

02 По возможности дайте ощущение уверенности в завтрашнем дне для вашего персонала – по крайней мере, ключевым сотрудникам. Лучше на деле (сохранив материальную компенсацию за труд на время вынужденного бездействия) или хотя бы на словах. Пандемия когда-нибудь закончится, а запрос на социальное ответственное поведение бизнеса останется. И если бизнесу суждено работать в пост-коронавирусные времена, сотрудники понадобятся.

03 Создайте исходящий информационный поток внутренних коммуникаций. Не надо непрерывно бомбардировать людей хрониками апокалипсиса. Достаточно стандартных напоминаний о правилах «коронавирусной гигиены», а остальную часть сообщений вполне можно сделать просветительскими и умеренно оптимистичными.

04 Помогите, чем можете, борьбе человечества с невидимым врагом. Само собой, у каждого бизнеса своим отношения с властью и свои приоритеты. Но отсидевшихся в тылу этого фронта после победы ждут репутационные потери, а не дивиденды. По крайней мере, помогайте власти транслировать правила выживания в условиях пандемии.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

05 Интернет-страницы в соцмедиа и сайт должны быть живыми, офисные телефоны и мэйлы основных подразделений (включая PR-службу) – отвечать.

06 Не молчите о том, как планируете работать с учетом изменившейся внешней среды ведения бизнеса. В любом случае, вы так или иначе строите планы применения интернета, меняете логистические модели, ищите новые ниши. И вполне возможно об этом поговорить хотя бы посредством соцсетей для малого бизнеса или посредством более охватных медиа, если есть возможность. В разумных пределах, естественно, не раскрывая своих внезапных инсайтов и коммерческих секретов.

07 Найдите способ убедить своих потребителей в том, что Вы можете им быть полезны в сложную минуту. У каждого бизнеса свой путь, ищите его в русле этой парадигмы.

08 Участвуйте в онлайн-ивентах под эгидой отраслевых ассоциаций и власти – это хороший способ быть заметными без лишних расходов и общаться с лидерами мнений.

09 Не только учите сотрудников правилам кибергигиены, но и соблюдайте их сами. Позаботьтесь о кибербезопасности корпоративной антикризисной переписки членов PR-команды – особенно в части общения с аутсорсерами (см. Рекомендации Комитета Киберустойчивости Бизнеса АПКБУ и Комитета Технических Средств Безопасности и Защиты Информации АПКБУ);

10 Если оказываете благотворительную помощь, то во внешних коммуникациях избегайте обещаний, реализация которых не полностью зависит от ваших усилий. Придерживайтесь принципа «сделано - сказано».

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

5. ОРГАНИЗАЦИЯ ЛИЧНОЙ ЖИЗНИ

Рекомендации от Комитета Психологической Безопасности

Целью Комитета психологической безопасности является развитие области управления психологическими корпоративными рисками в украинском бизнесе. В арсенале нашей команды собраны новейшие методики и техники из сферы корпоративной психологии и психодинамического организационного консультирования. В сферу нашей деятельности входят такие направления, как индивидуальный глубинный психологический ассессмент, глубинная диагностика организационных процессов, работа с сопротивлением изменениям в организации, групповая работа по улучшения командного взаимодействия, индивидуальное психологическое консультирование, executive коучинг, программы лидерского развития, тренинги, тестирование и многое другое.

Сегодня мы имеем дело с пандемией на двух уровнях – физиологическом и психологическом. Поэтому важно заботиться о своей базовой безопасности, своих близких и обществе также на этих двух уровнях.
На физическом уровне важно соблюдать все правила и рекомендации, которые мы получаем через официальные ресурсы МОЗ для предотвращения распространения инфекции. Но в то же время, существует и психическое массовое заражение, которое приводит к эпидемии страха и паники и негативно влияет на психоэмоциональные состояния каждого из нас. Все мы знаем насколько пагубно стресс влияет на состояние иммунитета. Вот несколько ключевых рекомендаций для поддержания психологического благополучия как своего, так и своей семьи.
Оценить границы своих возможностей и определить, на что Вы можете сейчас влиять, а на что – нет.
Направить своё внимание и действия только на то, на что Вы можете влиять. А именно:

01 Соблюдая все правила карантина, Вы предотвращаете распространение вируса. Соблюдая правила информационной гигиены, Вы предотвращаете распространение паники и ужаса. Не тратьте своё время на поиск пугающей информации о COVID-19 (особенно из недостоверных источников) и ни в коем случае не распространяйте ее дальше. Не вступайте в споры и баталии в комментариях, они отнимают большое количество психических ресурсов, которые сейчас так нужны.

02 Поддерживайте близкие отношения с родными и друзьями, общайтесь с ними онлайн. Отношения играют важную роль в нашей жизни. Доказано, что безопасная эмоциональная связь снижает физиологические показатели стресса.

03 Создайте структуру в своей повседневной жизни: создайте расписание для каждого члена семьи, соблюдайте распорядок дня, режим питания, распределите домашние дела между всеми членами семьи. Организованность и структура снижает уровень хаоса, и, как следствие, уровень тревоги.

АПКБ
АСОЦІАЦІЯ ПРОФЕСІОНАЛІВ КОРПОРАТИВНОЇ БЕЗПЕКИ

04 Добавьте физические упражнения. Двигательная и моторная активности эффективно способствуют отводу нервного напряжения. Так Вы поможете организму избавиться от гормона стресса – кортизола, а взамен получите дофамин – гормон, который отвечает за хорошее настроение.

05 Соблюдайте один и тот же режим сна и бодрствования. Старайтесь ложиться вовремя. Сон – главный регулятор гормональной системы, от его качества существенно зависит состояние иммунитета.

06 Занимайтесь интеллектуальным трудом. Мышление стимулирует работу областей головного мозга, отвечающих за саморегуляцию. Изучение языков, чтение книг, игры на логику и память – это не только приятное времяпрепровождение, но и способ справляться с негативными эмоциями.

07 Договоритесь со своими родными о возможности личного времени и пространства для каждого члена семьи. Соблюдайте личные границы друг друга.

08 Принимайте участие в организации помощи другим людям, вступайте в группы тех, кто уже это делает. Чувство сопричастности помогает снизить тревогу, а помощь другим даёт возможность действовать проактивно, что в свою очередь снижает чувство беспомощности.

09 Если Вы чувствуете, что Вы или члены Вашей семьи не справляются, и все вышеперечисленное не помогает – обращайтесь за помощью к специалистам, сейчас консультации широко доступны онлайн.