НАБОР ИНСТРУМЕНТОВ ИКАО ДЛЯ БОРЬБЫ С ИНСАЙДЕРСКОЙ УГРОЗОЙ

ОБЩИЕ ПОЛОЖЕНИЯ

Данный набор инструментов, созданный Рабочей группой по подготовке Группы экспертов по авиационной безопасности, призван помочь организациям, работающим в авиационной среде, лучше реагировать на постоянно меняющуюся инсайдерскую угрозу. Как отмечается в *Заявлении ИКАО о глобальном контексте риска в области авиационной безопасности* (Doc 10108 – Restricted), террористы постоянно стремятся воспользоваться уязвимыми местами в системах обеспечения контроля за безопасностью и совершать акты незаконного вмешательства (AUI) против авиации, чему может способствовать привлечение инсайдеров.

Кто такие инсайдеры?

Инсайдеры — это сотрудники, занятые полный или неполный рабочий день (включая подрядчиков, временный и самозанятый персонал), которые работают в авиационном секторе или обслуживают его и функции которых предусматривают для них привилегированный доступ на охраняемые объекты, к охраняемым предметам или к конфиденциальной информации о безопасности.

Что представляет собой инсайдерская угроза?

Под инсайдерской угрозой понимается риск, возникающий в результате проведения авиационным персоналом актов незаконного вмешательства или пособничества им за счет использования разрешенного им доступа, дающего им тактическое преимущество.

Чем объяснить поведение инсайдера?

Инсайдеры могут проводить или способствовать проведению AUI в силу недостаточной осведомленности, самоуспокоенности или злонамеренности. Неосведомленность о политике и процедурах и самоуспокоенность (безответственный подход к политике и процедурам) могут привести к тому, что инсайдеры непреднамеренно будут способствовать AUI из-за своей небрежности, бездействия или несоблюдения политики и процедур обеспечения безопасности.

С другой стороны, злонамеренные инсайдеры, принимающие сознательное решение о проведении AUI, могут пойти на это по причине личных проблем в сочетании с жизненными событиями и ситуационными факторами, такими как финансовая выгода, идеология, месть, стремление к славе или принуждение.

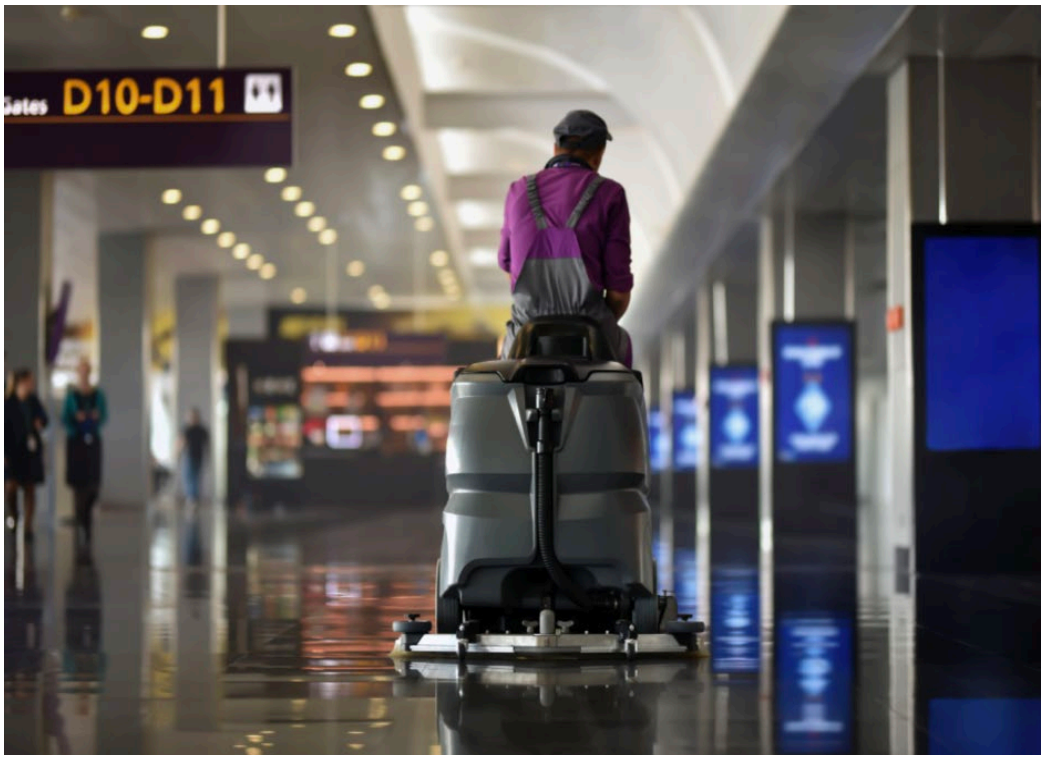
Злонамеренный инсайдер может умышленно попытаться поступить на работу в организацию для проведения AUI или прийти к намерению провести AUI в процессе своей работы (например, вербовка третьей стороной для использования инсайдера, пользующегося доверием).

Как действуют инсайдеры?

Инсайдеры могут проводить любые AUI (например, уничтожение воздушного судна в эксплуатации, пронос оружия или опасного устройства или материалов, предназначенных для преступных целей, на борт воздушного судна или в аэропорт). Инсайдеры могут обмениваться конфиденциальной информацией, содействовать доступу к зонам ограниченного доступа, неадекватно выполнять свои функции, позволяя вносить запрещенные предметы в зоны ограниченного доступа, помогать внешним сторонам получать доступ к компьютерным системам или другой цифровой инфраструктуре[1] и пр.

МЕРЫ ПО СНИЖЕНИЮ РИСКА

Ряд мер и правил обеспечения благонадежности персонала может помочь организациям уменьшить угрозу, исходящую от инсайдеров. В целом эти меры направлены на уменьшение риска найма сотрудников, которые могут представлять угрозу для безопасности в результате своих действий; на сведение к минимуму вероятности того, что действующие сотрудники станут представлять угрозу для безопасности; на снижение риска инсайдерской деятельности; и на защиту активов организации.



[1] Цифровая инфраструктура означает активы, в первую очередь касающиеся мобильной или интернет-связи.

Меры и инструменты по снижению инсайдерской угрозы можно сгруппировать по следующим направлениям.

ПРОВЕРКА АНКЕТНЫХ ДАННЫХ И ПРОВЕРКА НА БЛАГОНАДЕЖНОСТЬ

Политика и процедуры: надежная политика и процедуры проверки анкетных данных, включая личность сотрудника, предыдущий опыт работы, отсутствие судимости и образование, являются краеугольным камнем любой системы, направленной на снижение угрозы, создаваемой инсайдерами. Такие политика и процедуры должны быть четкими и краткими и периодически пересматриваться.

Исходные проверки анкетных данных: все сотрудники, которым необходим несопровождаемый доступ в контролируемые зоны и охраняемые зоны ограниченного доступа, а также лица, имеющие доступ к конфиденциальной информации о безопасности, должны пройти проверку анкетных данных[2] в соответствии с указаниями соответствующего органа.

Исходные проверки анкетных данных должны охватывать:

- удостоверение личности (например, предоставление паспорта, удостоверения личности, свидетельства о рождения и пр.);
- сведения о судимости (в полном объеме, разрешенном местными нормативными актами и законами);
- проверку послужного списка (для подтверждения добросовестности и общей пригодности потенциального сотрудника);
- сведения о трудовой деятельности (например, предыдущие работодатели, образование и пр.).

Повторные проверки анкетных данных: повторные проверки анкетных данных должны проводиться регулярно в рамках циклических проверок обеспечения благонадежности персонала. Рекомендуется проводить повторную проверку анкетных данных каждый раз, когда необходимо продлевать аэропортовые пропуска.

Те, кто совершают незаконные действия или AUI, пользуясь инсайдерским доступом или знаниями, часто приходят к такому намерению после приема на работу. Кроме того, многие инсайдеры, могут, возможно, ранее привлечь внимание руководства (например, из-за нарушения дисциплины и неудовлетворительных производственных показателей), что следует принимать во внимание в процессе повторных проверок анкетных данных.

Постоянные проверки на благонадежность: следует поощрять непрерывный процесс проверок в сотрудничестве с соответствующими полномочными органами (и, в соответствующих случаях, с полномочными органами других государств). Это необходимо для того, чтобы оценить, продолжает ли сотрудник соответствовать действующим должностным требованиям.

[2] Стандарт 3.5.2 Приложения 17 *"Авиационная безопасность"* (12-е издание, поправка 18)

Расширенные проверки анкетных данных: могут быть полезны проверки анкетных данных, охватывающие оперативные данные (и любую другую имеющуюся соответствующую информацию о пригодности человека к работе в той или иной должности). Несомненно, государства могут сотрудничать с соответствующими компетентными национальными органами в целях включения некоторых дополнительных данных в процесс многоуровневой проверки анкетных данных и проверки благонадежности.

Аналогичным образом, если сотрудники выявляют подозрительное или необычное поведение того или иного лица, то следует связаться с соответствующими органами безопасности и местными компетентными органами, поскольку может возникнуть необходимость в расширенной проверке анкетных данных с использованием оперативной информации.

ОБУЧЕНИЕ И ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ

Обучение в целях повышения осведомленности. Всех сотрудников следует поощрять проходить обучение для повышения осведомленности о мерах и культуре безопасности. Это поможет обеспечить знание всеми сотрудниками политики, стандартов, инструктивных указаний и процедур в области безопасности, а также понимание их целей по поддержанию высокого уровня безопасности. Такое обучение также позволит новым сотрудникам развивать способности по выявлению подозрительного поведения и безопасному информированию об этом соответствующего полномочного органа или правоохранительного органа/ведомства, в том числе обезличенными средствами.

Интеграция обучения. Повышение осведомленности по вопросам безопасности можно интегрировать в первоначальную подготовку и существующую периодическую переподготовку или с помощью агитационных материалов, практикумов, открытых занятий и пр. содействовать формированию прочной и эффективной культуры безопасности в авиации.

Обучение по вопросам, связанным с выполнением конкретных функциональных обязанностей. Для некоторых категорий персонала, включая, в частности, руководителей разных уровней и лиц, выполняющих обязанности в области обеспечения благонадежности персонала, целесообразно проводить более всестороннее обучение по вопросам, связанным с выполнением конкретных особенностей, чтобы обеспечить заданные результаты обучения.

Кампании повышения осведомленности. Следует подготовить графические сообщения, охватывающие ключевые аспекты безопасности, для размещения в организациях и аэропортах визуальных напоминаний для персонала.

МЕРЫ ПО КОНТРОЛЮ ДОСТУПА

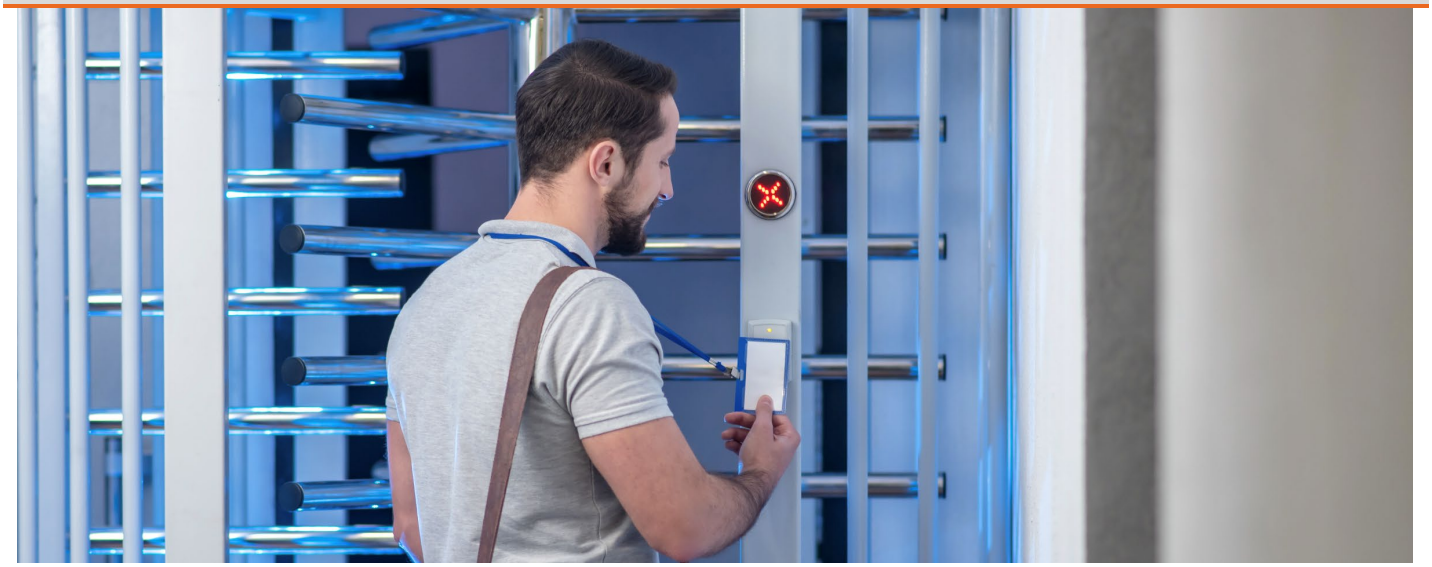
Досмотр. Необходимо принять меры по контролю доступа для проведения досмотра лиц, не являющихся пассажирами, и проносимых ими предметов до входа в охраняемые зоны ограниченного доступа[3]. Такой досмотр должен предусматривать некоторые выборочные и непредсказуемые методы досмотра, чтобы помочь нивелировать инсайдерские знания и уменьшить вероятность попадания запрещенных предметов в контролируемую зону, в том числе при проносе сотрудниками.

Правила и процедуры. Правила и процедуры должны быть четкими и включать в себя следующие:

- прекратить действие именных пропусков сотрудников, уволившихся из организации (например, ушедших в отставку, вышедших на пенсию и пр.);
- ограничить права лиц, имеющих пропуска, в отношении доступа в зоны ограниченного доступа, основанные на строгом принципе производственной необходимости;
- надлежащим образом охранять периметр и пункты контроля доступа для обеспечения того, чтобы нельзя было избежать проверки персонала в целях обеспечения безопасности;
- внедрить протоколы надзора и более широкое использование замкнутой телевизионной системы (ЗТС) для оперативной деятельности, где это необходимо.

[3] Стандарт 4.2.5 Приложения 17 *"Авиационная безопасность"* (12-е издание, поправка 18)

Пересмотр списков доступа. Рекомендуется пересматривать процедуры выдачи удостоверений личности, чтобы убедиться в том, чтобы сотрудник, запрашивающий доступ в определенный район, имеет производственную необходимость в таком доступе.



ПАТРУЛИРОВАНИЕ

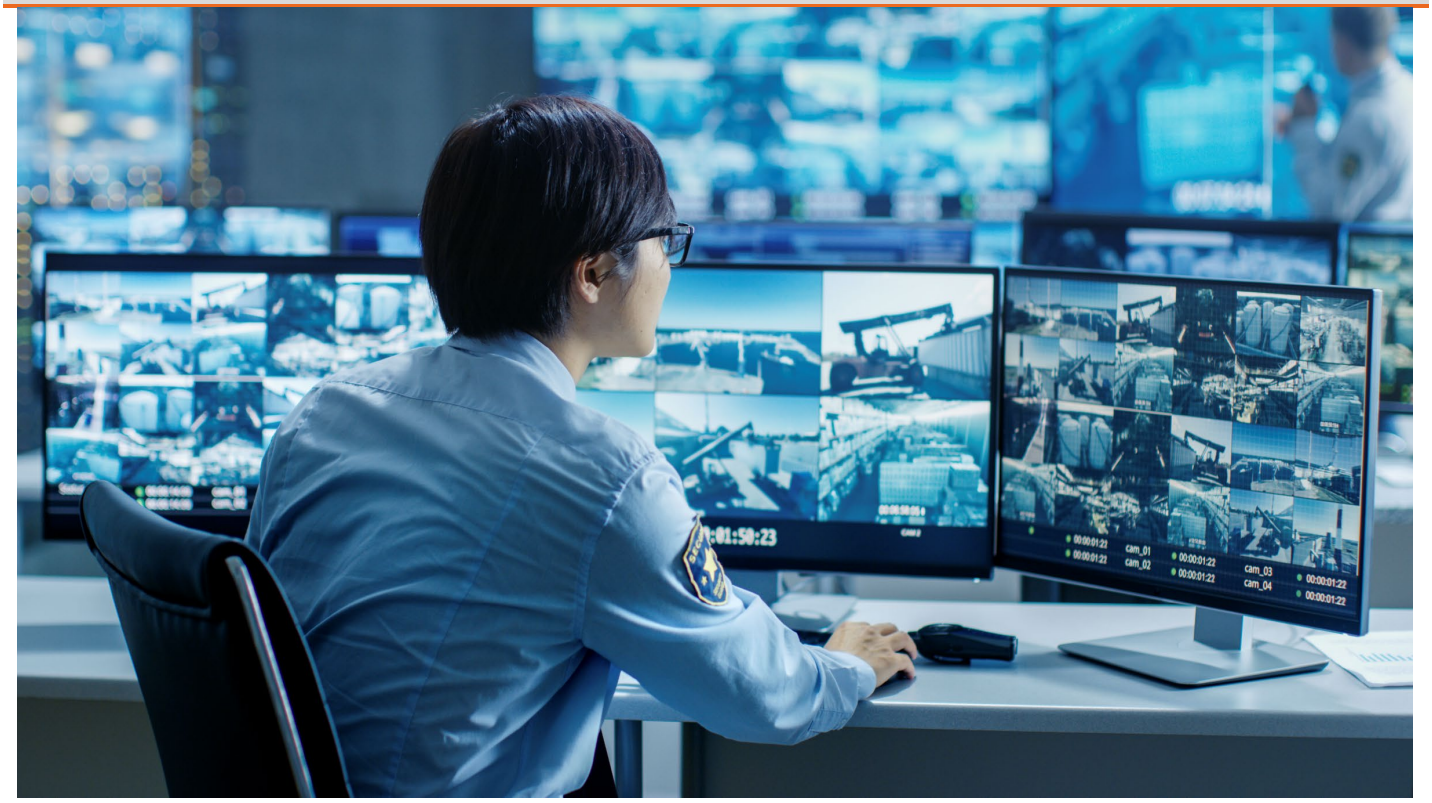
Выборочное и непредсказуемое. Должно осуществляться выборочное и непредсказуемое патрулирование (например, выборочные проверки), с тем чтобы в результате наблюдения лицам со злонамеренными целями или инсайдерскими знаниями нельзя было избежать патруля или обойти его. Кроме того, патрулирование должно быть направлено не только на наблюдение за персоналом аэропортов, но и за пассажирами, другими заинтересованными сторонами в аэропортах, а также за инфраструктурой аэропортов и товарами в целях выявления признаков необычной деятельности или недостаточного уровня обеспечения безопасности.

Патрулирование может быть эффективным визуальным средством сдерживания, если персонал носит форму и использует транспортные средства с маркировкой. Кроме того, скрытно осуществляемое патрулирование может обеспечить усиленный надзор.

НАБЛЮДЕНИЕ И МОНИТОРИНГ

Методы. Контроль качества, а также контроль за специфическими процессами и сотрудниками, связанными с инсайдерской угрозой, может играть важную роль в предотвращении или быстром урегулировании инцидентов в области безопасности и актов незаконного вмешательства. Методы контроля включают в себя замкнутую телевизионную систему (ЗТС), проверку регистрации доступов в систему (например, запросов на доступ) и наблюдение, осуществляемое персоналом на местах.

Руководители также играют важную роль в выявлении необычных видов деятельности и в контроле за поведением своих подчиненных.



Данные. В некоторых организациях данные о сотрудниках можно найти в различных журналах программных приложений, в которых указываются действия сотрудников. Эти цифровые данные могут отражать характер работы и использоваться в качестве инструмента для определения каких-либо преступных намерений со стороны сотрудников аэропорта (например, проходы в зоны без производственной необходимости).

Приложения могут включать в себя:

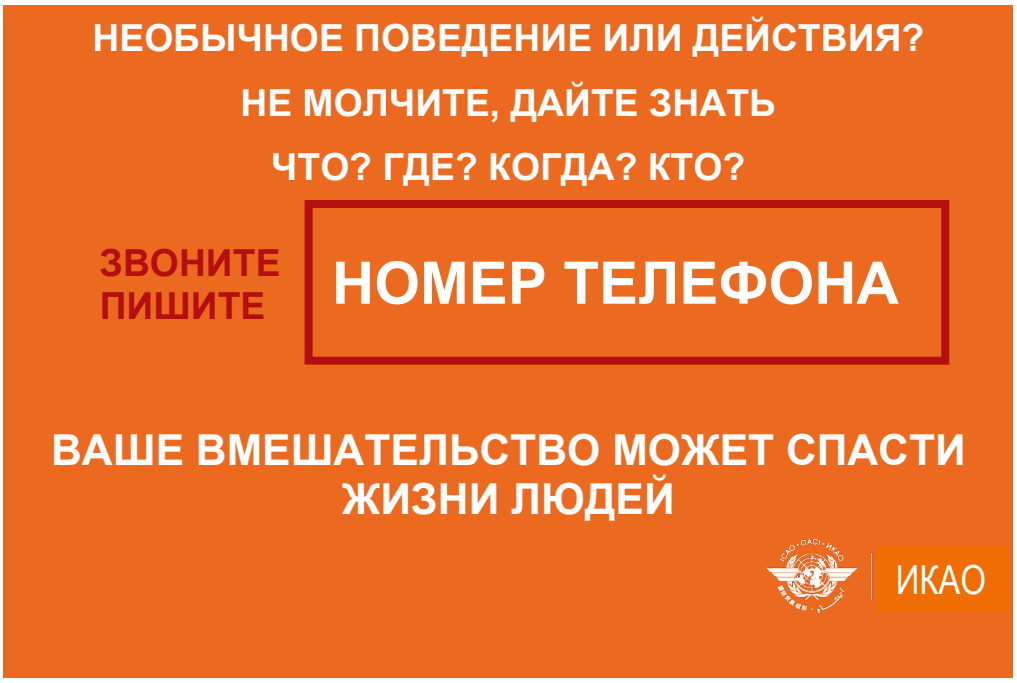
- журналы фактического входа/выхода, в которых основное внимание уделяется временному фактору и доступу к физическим пространствам;
- записи регистрации/выхода из системы с уделением особого внимания учетным данным, соответствующим срокам и пользователям;
- журналы приложений электронной почты;
- журналы приложений базы данных.

МЕХАНИЗМЫ ПРЕДОСТАВЛЕНИЯ ДАННЫХ

Сообщения о случаях подозрительного поведения. Механизмы отчетности должны охватывать всех членов организации, а не только тех, кто непосредственно занимается вопросами безопасности. Это важно, потому что сотрудники — это "глаза", "уши" и "голос" организации.

Механизмы представления данных могут быть устроены таким образом, чтобы сотрудники могли безопасно сообщать о подозрительном поведении или инцидентах посредством текстовых сообщений, электронной почты, телефонных звонков, по каналам внутренней связи или в ходе личного общения. На сообщения о состоянии безопасности следует давать четкий, эффективный и быстрый ответ.

Анонимные или конфиденциальные сообщения могут быть очень полезными для уменьшения потенциальных инсайдерских угроз и создания эффективной культуры безопасности в организации.



ВЫЯВЛЕНИЕ ПОВЕДЕНЧЕСКИХ ХАРАКТЕРИСТИК[4]

Выявление поведенческих характеристик. Полезным инструментом для уменьшения инсайдерской угрозы может быть выявление поведенческих характеристик. Оно основано на допущении о том, что люди могут демонстрировать признаки подозрительного или необычного поведения и эти признаки могут быть выявлены людьми, прошедшими надлежащую подготовку.

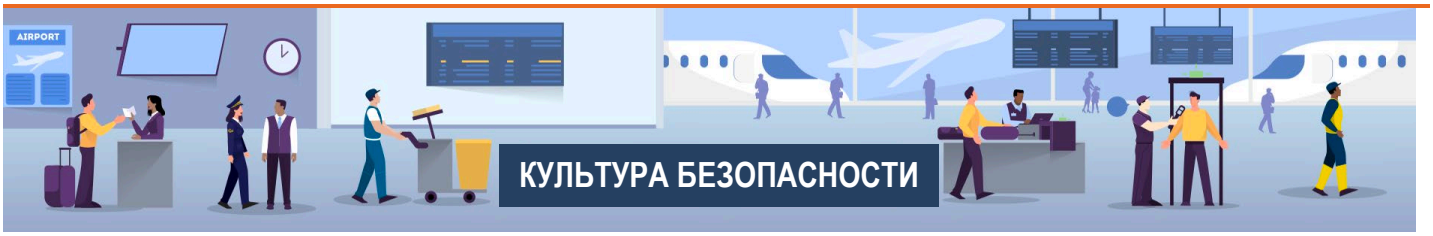
Подготовка кадров. Полезным инструментом может быть понимание сотрудниками того, что является подозрительной деятельностью и необычным поведением, а также понимание того, как сообщать об этом.

Обучение методам выявления поведенческих характеристик должен проходить широкий круг сотрудников, включая, в частности, тех, кто занимается выдачей пропусков, проведением проверок анкетных данных и досмотром. При этом все сотрудники могут получить пользу от такого обучения в рамках общей подготовки в целях повышения осведомленности по вопросам безопасности.

КУЛЬТУРА БЕЗОПАСНОСТИ[5]

Надежная и эффективная культура безопасности. Формирование позитивной культуры безопасности во всем авиационном секторе имеет важное значение для снижения уровня инсайдерских угроз и достижения эффективных и надежных результатов в области обеспечения безопасности. Сотрудники могут быть:

- мотивированы и информированы об инсайдерских рисках посредством регулярных брифингов по угрозам и более широким вопросам обеспечения безопасности;
- обучены выявлять и сообщать о необычном или подозрительном поведении;
- быть ценным источником информации об уязвимых местах и способах их устранения.



[4] Выявление поведенческих характеристик представляет собой применение методов распознавания поведенческих характеристик, включая, в частности, физиологические признаки или жесты, свидетельствующие о необычном поведении (сочетание вербальных и невербальных признаков) для выявления лиц, потенциально намеревающихся совершить акты незаконного вмешательства.
[5] Дополнительная информация о культуре безопасности (включая ресурсы ИКАО в области культуры безопасности) представлена на веб-сайте ИКАО, посвященном культуре безопасности, по адресу: www.icao.int/Security/Security-Culture

РУКОВОДСТВО И СТРАТЕГИЯ

Уверенная руководящая роль. Крайне важно, чтобы руководители понимали свою роль при демонстрации позитивных действий и поведения в области безопасности, ожидаемых от своих сотрудников. Следует поощрять открытый обмен информацией между сотрудниками и руководством, и руководители должны иметь представление о производственной повседневной нагрузке на персонал, а также об инсайдерских рисках, которые может создавать такая нагрузка.

Руководитель (например, старший менеджер), который берет на себя ответственность за обеспечение безопасности, применяет директивный подход к реализации принципов обеспечения безопасности и служит примером тому, как ожидаемое поведение сможет способствовать более гибкому и последовательному подходу во всей организации, что будет содействовать дальнейшему снижению уровня инсайдерских угроз.

Стратегия. Для того чтобы помочь сотрудникам понять, как распознавать подозрительное поведение на рабочем месте и сообщать о нем, рекомендуется использование стратегии предотвращения инсайдерских угроз (одобренной руководством).

Стратегия также может включать в себя связанные с персоналом положения об инсайдерах, руководящие принципы и процедуры. К ним относятся действия, которые должны быть предприняты до найма сотрудника и в течение всего времени его работы в организации. Стратегия и связанные с ней положения должны регулярно пересматриваться с участием всех ключевых заинтересованных сторон.

Рамочные документы[6], справочники и инструктивные материалы могут быть дополнительными полезными инструментами.

[6] Например, www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Возможности человека и человеческий фактор. Организации должны иметь представление о том, как работа человека может помочь снизить уровень инсайдерской угрозы. Это включает в себя осознание того, как человеческий фактор может влиять на людей, которые могут либо намеренно, либо непреднамеренно использовать свой уникальный доступ и стать причиной AUI. Руководители всех звеньев должны:

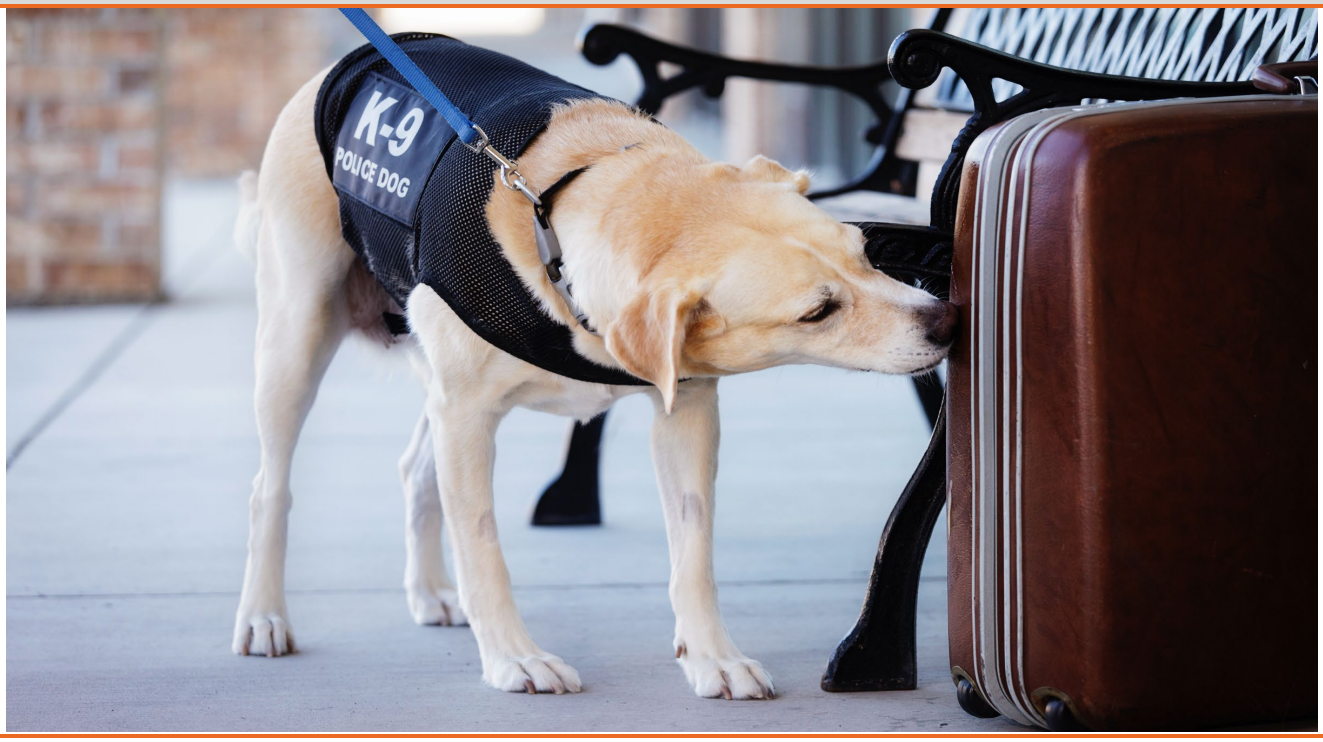
- развивать понимание человеческих способностей и того, как они могут помочь снизить риск инсайдерской деятельности;
- понимать человеческие ограничения и способы их корректировки для того, чтобы они не сказывались на эффективности работы;
- упрощать процесс сообщения сотрудниками информации о проблемах безопасности и подозрительном поведении;
- понимать связь между человеческим фактором, культурой безопасности и мотивацией;
- обеспечивать наличие ресурсов, необходимых персоналу;
- обеспечивать умение руководящего персонала выявлять признаки стресса и усталости, чтобы оперативно на них реагировать;
- избегать самоуспокоенности в повседневной деятельности.

ПЕРЕДОВЫЕ ТЕХНОЛОГИИ[7]

Обнаружение следов взрывчатых веществ (ETD). Использование оборудования ETD может обеспечить дополнительный уровень безопасности в придачу к стандартным процедурам досмотра пассажиров и/или выборочным и непредсказуемым мерам обеспечения безопасности, применяемым во всей охраняемой зоне ограниченного доступа, тем самым помогая снизить уровень инсайдерской угрозы.

[7] Применение современных технологий выборочно и непредсказуемо на всей территории аэропорта может способствовать снижению уровня инсайдерского риска за счет повышения уровня стандартов обнаружения в ходе процесса досмотра в целях безопасности и/или за счет создания дополнительных уровней обеспечения безопасности помимо базового уровня.

Собаки, используемые для обнаружения взрывчатых веществ (EDD). Группы EDD могут использоваться для многих целей, таких как: проверка в целях обеспечения безопасности во всех зонах аэропорта (неконтролируемая, контролируемая, зона проверки пассажиров, лиц, не являющихся пассажирами, багажа, грузов и пр.), досмотр охраняемой зоны ограниченного доступа и предоставление средств проведения выборочных и непредсказуемых мер безопасности.



Искусственный интеллект (ИИ). Использование систем на основе ИИ обученными сотрудниками может помочь выявить тенденции и необычную деятельность. Например, современные решения по управлению инцидентами могут помочь выявить инциденты и отличить обычные события от нависших угроз, таких как попытки проникновения в охраняемые зоны.

— КОНЕЦ —