МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ АЭРОПОРТОВ ОТ КИБЕРИНЦИДЕНТОВ

Аллаберганов Б.А.
Главный специалист отдела цифрового развития Министерства информационных технологий и коммуникаций Республики Узбекистан
Абдуллаев Д.Ш.
Степень магистра, Факультет кибербезопасности , Ташкентский университет информационных технологий имени Мухаммада аль-Хоразмий, Узбекистан

Абстрактный. *В сегодняшнюю информационную эпоху правительственные организации и коммерческие предприятия в значительной степени полагаются на взаимосвязанные компьютерные системы для управления различными общественными услугами, включая энергетику, транспорт, водоснабжение и т. д. Хотя это расширение возможностей подключения дает много эксплуатационных преимуществ, приносящих пользу населению, они также становятся уязвимыми. к кибератакам, таким как нарушения корпоративной безопасности, целевой фишинг и мошенничество в социальных сетях. Авиационный сектор является одной из важнейших инфраструктурных систем, которая уязвима не только для физических угроз , но и для киберугроз, особенно в связи с более широким использованием в аэропортах принципа «принеси свое собственное устройство» (BYOD). Было признано, что в настоящее время для аэропортов в Соединенных Штатах не установлены стандарты кибербезопасности, поскольку существующие стандарты в основном сосредоточены на системе управления воздушным судном (CS). В этом документе обобщаются потребности, предпосылки, текущие разработки и исследовательские усилия в отношении установления стандартов кибербезопасности и передовой практики в аэропортах США с особым акцентом на образование и грамотность в области кибербезопасности.*

Ключевые слова. *Аэропорт, критическая инфраструктура, безопасность, кибербезопасность, связь, сети, цифровые технологии, проникновение, уязвимость*

Введение. Авиация является подсектором транспортных систем S. сектор , один из 18 важнейших секторов инфраструктуры и ключевых ресурсов, определенных Президентской директивой № 7 (HSPD-7) по национальной безопасности США вместе с Национальным планом защиты инфраструктуры (NIPP). Среди всех видов транспорта отрасль авионики является одной из самых передовых в использовании стандартов кибербезопасности. Национальная система воздушного пространства (NAS) Федерального авиационного управления США (FAA) включает воздушное пространство США, аэронавигационные средства, оборудование, службы, аэропорты,

аэронавигационные карты, информацию/услуги, правила, положения, процедуры, техническую информацию, персонал и материал. FA совместно с Совместным планом я нг и Деве _ лопмент O f f ic e (JPDO) находится в процессе планирования и внедрения системы воздушного транспорта следующего поколения (NextGen), которая представляет собой эволюцию от наземной системы управления воздушным движением к спутниковой системе управления воздушным движением с более широкими коммуникационными соединениями. и услуги. Архитектура кибербезопасности NAS радикально меняется для поддержки реализации NextGen , заставляя весь сетевой трафик использовать одну из следующих классификаций трафика: внешняя граничная защита (EBP), сертифицированное управление программным обеспечением (CSM), обнаружение вторжений и реагирование (IDR) и внутренний Применение политики (IPE).

Материалы. В последней версии дорожной карты по обеспечению безопасности систем управления в транспортном секторе, подготовленной транспортным сообществом при содействии Национального отдела кибербезопасности (NCSD) Министерства внутренней безопасности США (DHS), Программа безопасности систем управления (CSSP), признается, что У NAS уже есть развитая программа кибербезопасности. Следовательно, «Дорожная карта» в первую очередь сосредоточена на системах управления, связанных с информационными службами авиакомпаний, информационно-развлекательными службами для пассажиров, которые в широком смысле называются системами управления воздушными судами (TSWG, 2020).

Методы. В «Дорожной карте» (TSWG, 2020) признается, что с появлением самолетов нового поколения с электронной поддержкой (таких как Boeing 787, Airbus A380 и т. д.) и беспрецедентного количества новых технологий, которые они поддерживают (например, IP- сети , Готовые коммерческие продукты [COTS], беспроводная связь, GPS) , уязвимости самолетов в кибербезопасности выросли в геометрической прогрессии. Точно так же двусторонняя передача критически важной информации между системами самолета и системами аэропорта через GateLink , беспроводные локальные сети (WLAN), сеть авионики с полнодуплексной коммутацией Ethernet (AFDX), системы мониторинга состояния и использования двигателя (HUMS) и электронные Полетные сумки (EFB) могут существенно повлиять на кибербезопасность как самолета, так и аэропортов (TSWG, 2021). Авиакомпании также осознали необходимость постоянного совершенствования стратегий информационной безопасности для защиты от киберугроз. Например, Boeing работает с авиационной отраслью и отраслью информационной безопасности над разработкой единой киберстратегии. Он также активно развивает Кибертехнический центр, который будет использоваться для проведения оценок киберугроз и уязвимостей, разработки киберзащиты для самолетов Boeing и, таким

образом, для поддержки потребностей в кибербезопасности своих клиентов-авиакомпаний (Rencher et al., 2020) .

Полученные результаты. В Соединенных Штатах насчитывается около 450 коммерческих аэропортов и 19 000 дополнительных аэропортов. В коммерческих аэропортах есть специальные зоны с разным уровнем безопасности, известные как охраняемые зоны, зоны отображения идентификации безопасности (SIDA), зона воздушных операций (AOA) и стерильные зоны (где пассажиры ждут посадки в вылетающий самолет после досмотра). SIDA и AOA обычно включают зоны загрузки багажа, зоны возле зданий терминалов и другие зоны рядом с припаркованными самолетами и объектами аэропорта. Обратите внимание, что некоторые эксплуатанты аэропортов могут обозначить все AOA как SIDA (GAO, 2019). Именно в силу самой системы аэропорты особенно уязвимы для внутренних и внешних киберугроз и атак со стороны преступников, террористов или иностранных субъектов (McAllister, 2021). Помимо традиционной ИТ-инфраструктуры, такой как электронная почта и Интернет, в сфере внутренних операций аэропорта существует несколько потенциальных целей для кибератак (McAllister, 2021):

• Системы контроля доступа и охраны периметра,
• авиационные системы с поддержкой eEnabled ,
• Системы управления учетными данными и документами (САПР, чертежи),
• Радарные системы,
• Наземный радар,
• Багажные системы с поддержкой сети,
• Беспроводные и проводные сетевые системы,
• HVAC, • Управление объектами,
• Коммунальные услуги,
• Диспетчерский контроль _ _ _ а ИСУ типа сбора данных (SCADA).

Сети аэропортов уязвимы для киберугроз по ряду причин (Cheong, 2011; Fortinet, 2012):

• USB-накопители,
• Ноутбуки и нетбуки,
• Беспроводные точки доступа,
• Различные USB-устройства (цифровые камеры, MP3-плееры и т. д.),
• Сотрудники, одалживающие чужие машины или устройства,
• Человек-троян (злоумышленники, которые посещают сайты под видом сотрудников или подрядчиков),
• Оптические носители (CD, DVD и т.д.),
• Отсутствие бдительности сотрудников,
• Смартфоны,
• Электронная почта,
• Социальные сети,

• Целевые атаки ботнетов,
• Взлом кликов и веб-атаки с использованием межсайтовых сценариев,
• Распределенные атаки типа «отказ в обслуживании» (DDoS),
• Проблемы облачных вычислений,
• Эксфильтрация данных и внутренние угрозы,
• Интернет-мошенничество.

В последние годы iPhone, iPad, Android , Планшет — обычное явление _ на рабочих местах, именуемой «Принеси свое собственное устройство» (BYOD). Эта тенденция набирает обороты и в аэропортах, где не только пользователи аэропортов, но даже персонал аэропорта хотят приносить свои собственные устройства на рабочее место. Однако, если эти устройства взаимодействуют с корпоративными системами (такими как электронная почта и доступ к VPN), они потенциально могут использоваться для тайного сбора конфиденциальной информации или распространения вирусов. Сотрудникам аэропорта нужны только корпоративные учетные данные для входа в систему, чтобы иметь возможность подключать свои неутвержденные личные устройства даже к защищенной сети WPA2/802.1x, не требуя разрешения администратора и подвергая сеть угрозам безопасности. Недавний опрос ИТ-специалистов, проведенный AitTight Networks, выявил серьезные проблемы безопасности, связанные с неуправляемыми личными устройствами, т. е. BYOD (AirTight , 2020). Система предотвращения вторжений в беспроводную сеть (WIPS), контроль доступа к сети (NAC) и управление мобильными устройствами (MDM) были определены как некоторые технологии для борьбы с все более распространенной угрозой подключения неуправляемых устройств к корпоративным сетям. Точно так же растущее использование мобильных точек доступа Wi-Fi может представлять серьезную киберугрозу, поскольку аппаратные средства для мобильных точек доступа, такие как устройства Mi -Fi и USB-маршрутизаторы Wi-Fi, могут быть легко доставлены в помещения аэропорта, а инструменты для создания программных точек доступа легко доступны. доступны на смартфонах сотрудников. Было подсчитано, что почти 20% корпораций в какое-то время имеют в своих сетях мошеннические точки доступа (AP), которые открывают сети для ряда целевых кибератак. Сотрудники могут неосознанно распространять вирусы и разрешать мошенническим пользователям доступ к корпоративным системам, посещая авторитетные веб-сайты (например, местную газету), переходя по ссылке в электронном письме, посещая сайты социальных сетей или вставляя зараженный USB-накопитель в свой компьютер или устройство. .

Заключение. Будущие интеллектуальные аэропорты будут иметь передовую коммуникационную инфраструктуру, которая будет поддерживать электронные самолеты в системе воздушного транспорта NextGen и предоставлять открытую платформу для сквозных услуг и приложений для всех, с повышенными рисками, связанными с киберугрозами. Хотя растущие риски, связанные с киберугрозами,

невозможно устранить, внедрение отраслевых стандартов, надлежащие меры кибербезопасности, передовой опыт и образовательная программа для всех сотрудников аэропорта (и пользователей) могут помочь смягчить их. Для защиты аэропортов от киберуязвимостей рекомендуется использовать эшелонированную защиту или подход «пояс и подвеска», когда для предотвращения всех потенциальных угроз не требуется полагаться на какой-либо один механизм безопасности. Кроме того, для устранения уязвимостей решающее значение имеет ориентированное на пользователя обучение кибербезопасности для всех сотрудников аэропорта, чтобы они знали о потенциальных угрозах, проводимые специальным персоналом по кибербезопасности. Агентства национальной безопасности признают, что борьба с киберугрозами является общей ответственностью, в которой важную роль должны сыграть государственный, частный и некоммерческий секторы, а также органы власти всех уровней. Таким образом, при выявлении и реагировании на аномальную деятельность аэропорты могут использовать свои существующие отношения с местными, государственными и федеральными правоохранительными органами, чтобы помочь им обеспечить надлежащее реагирование и решение.

Таким образом, несмотря на все достижения в области технологий, не существует панацеи для защиты ИТ-систем аэропортов от всех потенциальных киберугроз. В тех случаях, когда для предотвращения всех потенциальных угроз не требуется полагаться на какой-либо один механизм безопасности, рекомендуется использовать подход «глубокая защита » или «пояс и подтяжки». Конечно, при обеспечении безопасности сетей аэропортов потребности и эксплуатационные функции должны быть сбалансированы, чтобы требования безопасности не препятствовали работе, но в то же время обеспечивали безопасность критически важных операций и защищали от использования уязвимостей. Согласно Nessi (2020), многоуровневый подход к обеспечению безопасности, инвестирование в устройства Unified Threat Management (UTM), обеспечение безопасности всех конечных точек сети аэропорта, сохранение программных приложений, а также обновление прошивки в маршрутизаторах и коммутаторах, обеспечение соответствия данным индустрии платежных карт. Sec ur it y Sta нет данных rd (PCI-DSS), защита корпоративных баз данных, в которых хранится личная информация, в том числе информация о сотрудниках аэропорта и данные значков сообщества аэропортов, — все это важные меры, которые должны быть реализованы менеджером аэропорта с помощью ИТ-группы для защиты аэропортов от виртуальных уязвимостей. .

ССЫЛКИ:

1. АКИНА . 2021. План участия Комитета по бизнес-информационным технологиям ACI-NA. аэропорты Совет Международный из Север Америка . Доступный от Интернет : .

2. Воздухонепроницаемые сети. 2020. Влияние использования собственных устройств (BYOD) на корпоративную безопасность. Опрос _ к воздухонепроницаемый сетей , Inc. _ Доступный от Интернет : .

3. Кук, К. 2020. Терминал 5 аэропорта Хитроу: история успеха ИТ-инфраструктуры. аэропорты Международный Журнал , Ключ Издательский ООО _

4. Чеонг, Б. 2021. Кибербезопасность в аэропортах. Международный совет аэропортов Северной Америки. Доступный от Интернет : .

5. Дагган, Д.П. 2020. SAND2005-2846P: Тестирование промышленных систем управления на проникновение. Технические отчет , Сандия Национальный Лаборатории .

6. Фортинет. 2019. Топ-10 угроз сетевой безопасности. Fortinet, Inc. Доступно в Интернете : .

7. ГАО. 2019. Авиационная безопасность: национальная стратегия и другие действия усилят усилия TSA по обеспечению безопасности периметров коммерческих аэропортов и контроля доступа.

8. ГАО-09-399. Отчет для инициаторов Конгресса, Счетная палата правительства США (GAO), Вашингтон, округ Колумбия. Доступно в Интернете : .

9. Хан, А .; Крегель , Б.; Говиндарасу , М.; Фитцпатрик, Дж.; Аднан, Р.; Шридхар, С .; Хигдон, М. 2020. Развитие из в Безопасность PowerCyber SCADA испытательный стенд .