JIU/REP/2021/3

Организация Объединенных Наций

Кибербезопасность в организациях системы Организации Объединенных Наций

Доклад Объединенной инспекционной группы

Доклад подготовили *Хорхе Флорес Кальехас, Аиша Афифи* и *Николай Лозинский*

JIU/REP/2021/3
Russian
Original: English

Кибербезопасность в организациях системы Организации Объединенных Наций

Доклад Объединенной инспекционной группы

Доклад подготовили *Хорхе Флорес Каллехас, Айша Афифи* и *Николай Лозинский*

Организация Объединенных Наций • Женева, 2021 год

Коллектив сотрудников, работавших над докладом:

Хорхе Флорес Кальехас, Аиша Афифи, Николай Лозинский — инспекторы

Винсент Херми — сотрудник по оценке и инспекции

Сильвия Петкова — младший сотрудник по оценке и инспекции

Эрве Бода — помощник-референт

Деян Динчич — консультант

Шарлотта Клаво, Алина Дации, Бьянка Каневари — стажеры

Резюме

Кибербезопасность в организациях системы Организации Объединенных Наций

В современном цифровом мире кибербезопасность стала важным вопросом для международных организаций, и Организация Объединенных Наций не является исключением. Цифровая трансформация, растущая зависимость от информационно-коммуникационных технологий (ИКТ) и решений с киберподдержкой, а также тот факт, что киберугрозы постоянно растут, как по изощренности, так и по разрушительному потенциалу, привели к беспрецедентному увеличению рисков для кибербезопасности, с которыми сталкивается система Организации Объединенных Наций. Хотя кибербезопасность впервые появилась в сфере ИКТ, теперь, когда информационные системы нашли широкое применение в практике большинства организаций, а ландшафт угроз изменился настолько, что они уже не могут быть купированы лишь технологическими средствами защиты, уже не представляется возможным воспринимать кибербезопасность лишь через призму ИКТ. В настоящем докладе инспекторы аргументируют необходимость анализа соображений кибербезопасности как элемента более общих организационных процессов, таких как общеорганизационное управление рисками, планирование непрерывности деятельности, а также обеспечение безопасности и защиты, а также внимания к этой проблематике в масштабах всей организации.

В последние годы в системе Организации Объединенных Наций растет понимание того, что кибербезопасность требует внимания. В самом деле, потенциальные последствия недочетов в области кибербезопасности выходят за рамки нарушения работы инфраструктуры и систем ИКТ или объема данных, которые оказываются вскрытыми. Можно сказать, что на карту поставлены способность организаций системы Организации Объединенных Наций выполнять свои мандаты и их авторитет перед своими членами и партнерами. Более того, многие категории лиц, данные которых хранятся в организациях системы Организации Объединенных Наций, могут столкнуться с серьезными неблагоприятными последствиями в случае утечки этих данных. Хотя кибератаки могут по-разному влиять на организации с различными мандатами и структурами, их угроза реальна для всех из них. Ни одна организация не может ожидать, что никогда не столкнется с нарушением кибербезопасности, независимо от того, насколько она бдительна и насколько серьезно она подходит к защите от них. Кроме того, невнимание к рискам может иметь значительные репутационные, практические, юридические и финансовые последствия.

Цели настоящего обзора и структура доклада

Основные цели настоящего обзора: a) выявить и проанализировать общие проблемы и риски кибербезопасности, с которыми сталкивается каждая организация системы Организации Объединенных Наций, а также принимаемые этими организациями меры реагирования на них учетом конкретных требований организаций (вертикальная перспектива), и b) изучить нынешнюю межучрежденческую динамику, способствующую общесистемному подходу к кибербезопасности для улучшения координации, взаимодействия и обмена информацией между организациями системы Организации Объединенных Наций, а при необходимости и возможность общих решений (горизонтальная перспектива).

Основываясь на самооценке, предоставленной участвующими организациями, инспекторы сначала представляют в главе II моментальный снимок ландшафта кибербезопасности, как тот выглядит для системы Организации Объединенных Наций, описывая наиболее распространенные виды угроз и злонамеренного воздействия с указанием их сообщаемого воздействия и отмечая отдельные

технические вопросы, которые будут рассмотрены далее. В главе III инспекторы рассматривают институциональные механизмы и соответствующую практику в организациях системы Организации Объединенных Наций применительно к ряду ключевых элементов, выявленных в ходе обзора, которые способствуют киберустойчивости организации, и при необходимости выделяют передовой опыт. Глава IV посвящена межучрежденческому механизму укрепления координации и взаимодействия между организациями системы Организации Объединенных Наций и практическим возможностям разработки и реализации общих решения в области кибербезопасности там, где такие решения целесообразны. Среди экспертов имеется консенсус в отношении того, что ответные меры должны определяться спецификой и требованиями каждой организации (исходя из ее мандата, информации, которой она владеет или распоряжается, подверженности рискам, ресурсов и т. п.). В то же время организации системы Организации Объединенных Наций не действуют изолированно, а во многих отношениях взаимосвязаны, в том числе в результате совместной разработки и реализации ими программ и определенной степени взаимозависимости их мандатов и деятельности. Поэтому крайне важно определить области общей уязвимости, а также изучить области, в которых возможен согласованный подход.

Кибербезопасность в системе Организации Объединенных Наций

Ни одна организация системы Организации Объединенных Наций не может утверждать, что она не подвергалась в какой-либо форме кибератакам большей или меньшей серьезности. Вредоносные действия, направленные против пользователей информационных систем (такие как фишинг, кража личных данных, перехват канала связи и т. п.) или инфраструктуры (вредоносное ПО, распределенные атаки «отказ в обслуживании» и т. п.), на сегодняшний день являются наиболее распространенным источником ставших известными угроз. Хотя угрозы кибербезопасности обычно связаны с современными технологиями и программными решениями, экспертное сообщество видит заметный сдвиг от хакерских атак на серверы, сети и конечные устройства к атакам на людей с использованием методов социальной инженерии, направленных на манипулирование людьми с целью выманивания у них конфиденциальной информации для мошеннических или других незаконных целей. Пандемия коронавирусной инфекции (COVID-19) еще больше усугубила риски, связанные с социальной инженерией: более двух третей участвующих организаций сообщили о резком усилении угроз и уязвимостей кибербезопасности во время глобальных ограничительных мер, которые лишили многих пользователей доступа к централизованно управляемыми ресурсами кибербезопасности.

В то же время сообщаемое влияние инцидентов, с которыми столкнулись участвующие организации, было ограниченным, что может привести к преждевременному выводу об отсутствии серьезных причин для беспокойства. Это не тот вывод, к которому пришли инспекторы. Во-первых, собранные данные неизбежно предполагают наличие некоторых непросматриваемых зон, в том числе возникающих из-за понятного нежелания раскрывать известный уровень уязвимости и из-за непрозрачного характера киберактивности в целом, указывая на то, что точные масштабы угрозы и связанных с ней последствий может быть просто неизвестны. Чаще всего, особенно в случае более изощренных атак, злоумышленникам невыгодно раскрывать свое присутствие или использованные ими уязвимости, поэтому число проникновений в систему и утечек данных, вероятно, гораздо больше, чем сообщается. Доля «известных неизвестных» по сравнению с тем, что известно о масштабах угрозы кибербезопасности, велика, но доля «неизвестных неизвестных» может вызывать еще большее беспокойство. Таким образом, было бы ошибкой судить о серьезности угрозы по степени ее известной материализации в прошлом. Потенциал ущерба остается высоким и требует постоянного внимания и расстановки приоритетов.

Разница в зрелости организаций и отдельные аспекты технологической готовности

Настоящий обзор не претендует на всестороннюю оценку надежности рабочих механизмов или технической инфраструктуры каждой участвующей организации, а скорее призван дать представление об общих имеющихся возможностях и выделить некоторые общие проблемы, которые могут заслуживать особого внимания. По очевидным причинам, связанным с предметом настоящего обзора, инспекторы предпочли не раскрывать данные о системах конкретных организаций, поскольку это могло бы поставить под угрозу их безопасность. Принимая во внимание ограничения, характерные для информации, собираемой в основном с помощью самооценки, а также значительные различия в степени детализации данных, представленных респондентами, Объединенная инспекционная группа (ОИГ) отметила существенные различия в подходах участвующих организаций к реагированию на угрозы кибербезопасности и, как следствие, зрелости их доктрины кибербезопасности. Эти различия могут объясняться следующим: условиями, в которых действует каждая организация; требованиями, продиктованными характером хранимых данных; уровнем понимания и приоритетом, определяемым для кибербезопасности их руководством; историей становления данной организации; наличием ресурсов; а также большим разнообразием ИКТ-систем, инструментов и программных решений, используемых в масштабах системы.

Участвующие организации считали, что они хорошо понимают основные технические аспекты кибербезопасности и инвестировали соразмерно своим возможностям. Что касается технологического и рабочего потенциала, то в своем анализе инспекторы ограничились выделением ряда вопросов, которые, возможно, заслуживают более пристального внимания, например, следующих: сопряжение оконечных устройств и инструменты организации удаленной работы, в частности в условиях пандемии COVID-19; риски, связанные с рудиментами устаревших систем, приобретенных в прошлом или созданных своими силами с течением времени, которые могут больше не поддерживаться современными средствами проверки безопасности и решениями; продолжающееся расширение использования облачных вычислений; организационные механизмы анализа и преодоления уязвимостей; а также применение теневых информационных технологий (теневых ИТ), включая использование и реализацию технологических инструментов вне системы ИКТ организации. Следует отметить, что, несмотря на множество возникших проблем, пандемия также вызвала некоторые позитивные изменения. В силу безотлагательной необходимости подразделения Организации Объединенных Наций были вынуждены более внимательно изучить свои системы обеспечения безопасности и начали реализовываться запланированные организационные проекты ИКТ. Можно сказать, что массовый переход на удаленную работу в столь короткие сроки побудил многие организации активизировать свои усилия по повышению безопасности удаленного доступа и, возможно, придал столь необходимый импульс активизации действий в этом направлении.

Элементы, способствующие повышению киберустойчивости

Инспекторы изучили ряд элементов, способных улучшить состояние кибербезопасности организаций системы Организации Объединенных Наций и расширить их возможности выявления, предотвращения и обнаружения киберугроз, а также реагирования на инциденты и восстановления работы после них. Требуется многогранный подход, охватывающий все уровни организации: директивные и руководящие органы; механизмы надзора; административное управление; руководители среднего звена как административных, так и структурных или организационных единиц; а также сотрудники в целом. Кроме того, сквозная функциональность этой области требует более широкого взгляда, выходящего за рамки ИКТ и прямо вписывающего кибербезопасность в практику общеорганизационного управления рисками, а также стремления к большему сближению между физической безопасностью и кибербезопасностью. Наконец, что не

менее важно, кадры штатных специалистов в дополнение к сторонним поставщикам услуг, привлекаемых для решения конкретных, разовых задач, и финансовые ресурсы, выделенные соразмерно требованиям каждой организации, составляют основу надежной системы кибербезопасности. Итак, степень, в которой эти элементы отражены в подходе организации к кибербезопасности, прямо влияет на ее киберустойчивость. Поэтому инспекторы рекомендуют исполнительным главам начать проведение общеорганизационного обзора, чтобы изучить, в какой степени каждый из этих элементов, подробно рассмотренных ниже, встроен в политику и практику организации, и сообщить о результатах своим директивным и руководящим органам с целью получения указаний о том, как еще больше усилить киберустойчивость с учетом сильных и слабых сторон, выявленных в этом процессе (рекомендации 1 и 2).

Директивные и руководящие органы, обеспечивающие стратегическое руководство и ресурсы

В системе Организации Объединенных Наций кибербезопасность по-прежнему воспринимается как преимущественно технический вопрос, что может объяснить, почему степень привлечения директивных и руководящих органов к рассмотрению этой темы или ее вовлеченности в ее рассмотрение на сегодняшний день в большинстве организаций ограничена. В свете более широких аспектов кибербезопасности, определенных в настоящем докладе, инспекторы считают, что директивным и руководящим органам следует уделять более предметное внимание этому вопросу и давать стратегические указания высокого уровня, в том числе путем подготовки программного документа, четко фиксирующего допустимые пределы риска, и соответствующего распределения ресурсов, позволяющих достичь необходимой степени защиты. В более общем плане административное руководство должно размышлять о том, как регулярная отчетность по вопросам кибербезопасности для директивных и руководящих органов составляется и используется для налаживания взаимодействия с этими органами в пределах того, что может считаться необходимым и достаточным, без ущерба для защиты организации. Учитывая внезапный и потенциально серьезный характер киберинцидентов, инспекторы также рекомендуют организациям предвидеть необходимость доведения инцидентов до сведения директивных и руководящих органов, как внутри них, так и между членами самих таких органов, и предусмотреть процедуры на этот счет.

Внимание надзорных органов, способствующее усилению мер кибербезопасности

Было установлено, что механизмы внутреннего и внешнего надзора в организациях системы Организации Объединенных Наций внимательно относятся к вопросам кибербезопасности даже в отсутствие прямого упоминания этой темы как таковой в их мандатах. Инспекторы обнаружили несколько примеров совершенствования систем кибербезопасности участвующих организаций по рекомендациям надзорных органов (например, введение должности главного сотрудника по информационной безопасности, рекомендации по обучению, составление конкретной дорожной карты и т. п.). Комитеты по аудиту и надзору фактически рассматривают вопросы кибербезопасности в рамках своего мандата, охватывающего управление общеорганизационными рисками, а не в связи с организацией использования ИКТ. Похвально, что эти комитеты затрагивают эту тему не только для оказания помощи руководству, но и для информирования директивных и руководящих органов о соответствующих рисках для кибербезопасности, позволяя тем вносить свой вклад в снижение организационных рисков. Чтобы максимальную отдачу надзорных органов в области кибербезопасности, важно, чтобы знания и опыт экспертов по кибербезопасности в организации были востребованы в работе надзорных органов.

Нормативно-правовая база и контроль ее соблюдения

Участвующие организации называют разнообразные отраслевые стандарты кибербезопасности, иногда больше одного, при этом большинство из них либо уже прошли сертификацию по ИСО 27001, планируют это сделать, либо добровольно согласились привести свою систему в соответствие с этим стандартом, не запрашивая официальной сертификации. Инспекторы воздерживаются от аргументов в пользу одного отраслевого стандарта или согласованного общесистемного подхода в этом вопросе, поскольку разные стандарты могут действительно служить разным целям и давать необходимую возможность выбора с учетом разных уровней развития. Тем не менее есть веские основания черпать вдохновение — формально или неформально — в соответствующих отраслевых стандартах при создании собственной нормативно-правовой базы и ее использовании. Поэтому участвующие организации должны определить адекватный стандарт и, в рамках этого стандарта, наиболее подходящие средства контроля, исходя из уровня защиты, необходимого в свете их ситуации, в зависимости от требований и рисков, выявленных с помощью надлежащей оценки рисков для кибербезопасности данной конкретной организации.

Несколько ведущих отраслевых стандартов требуют наличия конкретных правил кибербезопасности и задокументированных процедур в качестве ключевого элемента контроля, лежащего в основе подхода организации к кибербезопасности. Можно сказать, что, за некоторыми исключениями, участвующие организации осознали важность наличия четкой системы норм, лежащих в основе их подхода к кибербезопасности. Стратегии высокого уровня в области ИКТ обычно включают соображения кибербезопасности, хотя и с разной степенью проработки. Более двух третей участвующих организаций разработали установочные документы, специально посвященные кибербезопасности, при этом три из них в настоящее время пересматривают их, а четыре находятся в процессе разработки специальной директивы. В то же время в четырех участвующих организациях функция кибербезопасности, включая соответствующую нормативно-правовую базу, считалась в лучшем случае находящейся на начальном этапе. Вопрос о соблюдении — в частности мерах воздействия в случае несоблюдения — действующих правил вселил меньшую уверенность в наличии корпоративной культуры кибербезопасности во всей системе. По мнению инспекторов, это требует более внимательного изучения и применения более нюансированных подходов к усилению ответственности за нарушения и защите организаций в целом.

Формирование культуры кибербезопасности сверху вниз

Первый шагом на пути к формированию культуры кибербезопасности — осознание самим высшим руководством связанных рисков и выработки понимания последствий плохой кибергигиены. Это влечет за собой более активную позицию со стороны руководителей высшего звена, добивающихся создания таких механизмов внутреннего управления, которые дают им необходимую информацию и фактологическую базу. В этом отношении роль руководства выходит за рамки принятия решений о распределении ресурсов. Главное здесь — поощрение внутренней культуры, в которой признание и активное отслеживание возникновения инцидентов воспринимается не как признание неудачи, а как отправная точка для совместного решения общей проблемы и усиления защиты организации и ее ресурсов. Другие способы, с помощью которых руководство может побуждать к действиям и конкретным образом влиять на образ мышления во всей системе подчиненности, — показывать модель рекомендуемого поведения, обеспечивать управленческую подотчетность во всей организации, участвовать в программах повышения осведомленности и демонстрировать активный стиль руководства в вопросах кибербезопасности в целом. В системе Организации Объединенных Наций необходим культурный сдвиг, и важное значение для него имеет вклад руководства, задающего тон на самом верху.

Восприятие кибербезопасности как общеорганизационной проблемы

В русле растущего понимания того, что ответственность за кибербезопасность не может лежать только на подразделениях ИКТ, большинство участвующих организаций так или иначе признали, что административные, а также оперативные подразделения должны играть здесь свою роль. Однако информация, собранная в ходе настоящего обзора, позволяет считать, все подразделения организаций, возможно, все еще недостаточно серьезно относятся к учету требований кибербезопасности и устойчивости при разработке и реализации своих проектов и мероприятий. Отмечалось, что в некоторых кругах правила и процедуры кибербезопасности рассматриваются как помеха для гибкости и эффективности деятельности, а не как щит, ограждающий репутацию и ресурсы организаций. Особенно важно, чтобы исполнительные главы активно противодействовали таким представлениям. Более четкое определение кибербезопасности как аспекта программных и административных функций может уменьшить недопонимание дополнительных ролей и обязанностей различных подразделений и устранить недостаточную вовлеченность некоторых заинтересованных сторон, выявленную в ходе настоящего обзора. Учет соображений кибербезопасности в политике и практике регулирования работы всех подразделений сам по себе будет признанием того, что каждая функция в организации может внести свой вклад в достижение общеорганизационного подхода в этом вопросе.

Персонал как первая линия защиты

Сохраняется проблема обучения каждого сотрудника его роли в защите информации и цифровых активов организации, а также важности соблюдения правил, процедур и рекомендованных стандартов кибербезопасности. Человеческий фактор приобрел значение не только в общем ландшафте угроз для кибербезопасности, что отражается в глобальной озабоченности по поводу того, что все больше им подвергаются отдельные конечные пользователи, но и как важный элемент в структуре защиты участвующих организаций при условии, что такие пользователи получают необходимую подготовку. Осознание того, что ответственность за киберзащиту начинается с хорошо информированных и бдительных пользователей, повлекло за собой большие усилия в плане инициатив по обучению и повышению информированности, несмотря на ограниченность ресурсов, усталость пользователей от обучения и трудности с тем, чтобы не отставать от последних веяний в этой динамичной области. Тем не менее эти многочисленные программы и отдельные инициативы, по-видимому, не реализовывались последовательно, систематически или с учетом рисков. Поэтому инспекторы рекомендуют организациям стремиться к разработке комплексной программы обучения и повышения информированности, продуманной на опережение как инструмент изменения внутренней культуры с помощью установления четких целей для каждой категории заинтересованных сторон в зависимости от рисков, которые могут быть связаны с ними для организации, а не предлагать каждому отдельные модули, не связанные стратегическим видением. Уделение внимания эпизодическим пользователям систем ИКТ организации, включая делегатов конференций, стажеров, посетителей и другие их категории помимо штатных сотрудников, имеет большое значение, поскольку такие пользователи часто входят в организационную инфраструктуру с личных устройств. Кроме того, будучи нечастыми пользователями этих систем, они с меньшей вероятностью будут осведомлены об их правильном и безопасном использовании в соответствии с применимыми правилами и практикой организации.

Оптимизация расходов на кибербезопасность и инвестиций в нее

Оценка ресурсов, выделяемых в настоящее время на кибербезопасность, представляет собой сложную задачу из-за особенностей финансовых и бюджетных процессов организаций системы Организации Объединенных Наций и их практики использования таких ресурсов и их учета. Само собой разумеется, что надежная система защиты кибербезопасности имеет свою цену. Несмотря на сообщения об

увеличении ресурсов, выделяемых на кибербезопасность, специалисты-практики в системе Организации Объединенных Наций по-прежнему воспринимают нехватку ресурсов как препятствие, не позволяющее их организациям охватить все аспекты киберустойчивости. Важно помнить, что сумма, потраченная на кибербезопасность, не отражает уровня защиты. Главное — даже не дискутировать о сумме затрат, а определить, на какие цели необходимо выделить ресурсы, чтобы получить максимум отдачи. Независимо от объема доступного финансирования собранная информация не указывает на последовательный подход к установлению организациями системы Организации Объединенных Наций приоритета расходов на кибербезопасность, что повышает риск неэффективного использования и без того скудных ресурсов. Для оптимизации расходов на кибербезопасность, а также связанных с ней инвестиций, необходима тщательная оценка киберрисков, завершающаяся экономическим обоснованием с подробным описанием затрат, выгод, рисков и ожидаемой экономии, а также показывающая потенциальные финансовые последствия отказа от инвестиций, которая станет условием поддержки и выделения адекватных ресурсов директивными и руководящими органами.

Внутренний экспертный потенциал кибербезопасности

Более половины участвующих организаций создали специализированный и предназначенный для данной цели кадровый потенциал, начиная от одного эксперта по информационной безопасности, иногда совмещающего эти задачи с другими, до целого организационного подразделения, возглавляемого главным сотрудником по информационной безопасности. Наоборот, в 10 участвующих организациях задачи кибербезопасности возлагаются в основном на специалистов по ИКТ наряду с другими их обязанностями. В области кибербезопасности часто привлекаются сторонние специалисты из-за ее технической сложности и постоянного развития, что требует во многом специальных знаний, которые сложно и дорого поддерживать в рабочем состоянии на постоянной основе. Обращение к сторонним структурам для наращивания и дополнения внутреннего потенциала неизбежно и даже желательно для того, чтобы оставаться в курсе быстро меняющихся событий в киберпространстве. Степень, в которой это делается, зависит от усмотрения каждой организации в свете ее задач и условий. Однако, по мнению инспекторов, организациям важно сохранять надлежащую степень контроля, надзора и технического потенциала внутри них для действенного использования потенциала, предоставляемого сторонними структурами, и взаимодействия с ним. В этой связи возможность поручить эти задачи специалисту — руководителю подразделения информационной безопасности может обеспечить нацеленность на надежное выполнение этой цели. Основные функции, составляющие сферу ответственности главного сотрудника по информационной безопасности, выходят за рамки разработки средств контроля на эксплуатационном уровне и по умолчанию включают управленческий аспект для обеспечения максимально полного отражения соображений кибербезопасности как вопроса управления общеорганизационными рисками и устойчивости к внешним воздействиям.

Отмечая различия во внутренней структуре, наблюдаемые в участвующих организациях, которые могут указывать скорее на их ограничения, чем на целенаправленный или стратегический выбор, инспекторы полагают, что наличие у организации занимающихся вопросам кибербезопасности специалистов способствует укреплению кибербезопасности в организации, а также во всей системе и такие затраты вполне заслуживают рассмотрения. Кроме того, каждой организации было бы целесообразно оценить, может ли она получить отдачу от создания центра безопасности, даже в самой базовой форме, проведя для этого анализ затрат и выгод для конкретной организации с такими параметрами, как сложность организационной инфраструктуры ИКТ, число и характер критически важных ресурсов и контролируемых процессов, общий объем потоков данных и, таким образом, периодичность угроз, а также другие факторы. Один из важных аспектов специально созданного центра безопасности, независимо от его размеров и штата, — нацеленность на ежедневный контроль процессов и выполнение важнейших функций координации и синхронизации, а также повышение информированности в

организации, что может существенно способствовать эффективности распределения внутренних ресурсов и функций.

Кибербезопасность — общесистемный приоритет?

Укрепление состояния кибербезопасности в системе Организации Объединенных Наций на основе усиления координации и взаимодействия между организациями на стратегическом уровне и расширения общесистемного оперативного потенциала провозглашалось на протяжении многих лет приоритетной задачей как государствами-членами, так и исполнительным руководством. Однако, несмотря на наличие в системе нескольких важных ресурсов, механизмов и инициатив, включая очевидную политическую волю, прогресс в реализации этих масштабных задач был менее чем очевиден. На сегодняшний день нет единого подразделения, которому было бы официально поручено продвигать повестку дня согласованного подхода к кибербезопасности, когда общесистемные усилия по обеспечению кибербезопасности в организационном плане строятся на межучрежденческих координационных механизмах под эгидой Координационного совета руководителей системы Организации Объединенных Наций и при оперативной поддержке, в определенной степени, Международного вычислительного центра Организации Объединенных Наций как поставщика общих услуг кибербезопасности для нескольких организаций системы Организации Объединенных Наций. В ходе настоящего обзора инспекторы выявили недостаточную увязку общесистемного стратегического целеполагания и оперативного потенциала, что повлияло на динамику между этими структурами и, вероятно, дорого обойдется системе с точки зрения нереализованного повышения эффективности из-за упущенных возможностей более непосредственного взаимодействия.

Необходимость базового уровня защиты и согласованных минимальных требований к ней

Общепризнано, что слабая защита от киберугроз в одной организации повышает уязвимость всей системы. Таким образом, можно сказать, что система Организации Объединенных Наций не прочнее ее самого слабого звена. Однако прежние инициативы, направленные на установление общих критериев или сравнительных оценок зрелости во всех организациях, не получили необходимой поддержки, когда их критики указывали на разнообразие структурных форм и условия деятельности организации как препятствие, ограничивающее ценность таких коллективных или общих подходов. Кроме того, участвующие организации не проявили особого интереса на высшем уровне к обмену своей внутренней информацией о кибербезопасности из соображений конфиденциальности и опасений по поводу раскрытия уязвимостей даже среди организаций. Эти опасения можно было бы уменьшить при помощи договоренностей об обмене информацией, которые могли бы предусматривать соответствующие гарантии. Однако попытки создать общесистемный функциональный потенциал для предотвращения и обнаружения киберугроз и реагирования на них еще не принесли ощутимых результатов. Некоторые из пробелов в этом отношении были заполнены Международным вычислительным центром Организации Объединенных Наций, чей портфель услуг кибербезопасности привлек значительную клиентскую базу, хотя получение таких услуг требует официального согласия организаций, в силу чего запросы системы могут быть удовлетворены лишь частично. Несмотря на ограниченный на сегодняшний день успех общесистемных усилий по выработке общего или согласованного подхода, будь то на концептуальном или рабочем уровне, инспекторы считают, что определение базового уровня защиты и минимальных требований к защите для организаций системы Организации Объединенных Наций и, следовательно, для системы в целом остается актуальной целью, к которой по-прежнему стоит стремиться.

Межведомственные механизмы кибербезопасности

Инспекторы отмечают, что межучрежденческий механизм кибербезопасности создан давно и в целом функционирует, хотя некоторые из масштабных целей, которые он перед собой поставил, еще не принесли осязаемых результатов, не считая активного обмена информацией и профессиональным опытом в рамках всей системы, налаженного благодаря ему. Документы Сети по цифровизации и технологиям и Комитета высокого уровня по вопросам управления показывают, что на протяжении как минимум 30 лет кибербезопасность занимает достаточно заметное место в повестке дня всей системы. С 2011 года Специальная группа по информационной безопасности, которая работает в рамках Сети по цифровизации и технологиям, служит основным механизмом развития межведомственного сотрудничества и взаимодействия с целью оптимизации информационной безопасности входящих в нее организаций. Согласно ее кругу ведения ее главная цель заключается в обмене информацией, однако после пересмотра этого круга ведения в 2018 году акцент также делается на ее роли в реализации совместных проектов — задача, которая была дополнительно усилена призывом создавшей ее Сети к Специальной группе по информационной безопасности активнее заниматься разработкой и внедрением совместных решений и инноваций. Признавая профессиональный авторитет и значительный объем работы, проделанной группой на протяжении многих лет, инспекторы пришли к выводу, что широкомасштабные совместные решения для системы не были реализованы в соответствии с ее мандатом. В качестве координирующего органа Специальная группа по информационной безопасности сталкивается здесь с теми же проблемами, что и любой другой межучрежденческий механизм, не имеющий полномочий по принятию обязательных к исполнению решений непосредственно на уровне системы, поэтому было бы нереалистично ожидать реализации таких решений от этого форума. Воздействие Специальной группы по информационной безопасности в некоторой степени ограничено ее зависимостью от участия и последующей деятельности каждой участвующей организации, разными полномочиями ее членов в их собственной институциональной архитектуре и тем, что у Группы нет практических возможностей выполнения достигнутых договоренностей или вынесенных рекомендаций. Кроме того, Группа отчитывается перед Сетью по цифровизации и технологиям, тем самым отражая организационную схему, типичную для большинства организаций, в которой главный сотрудник по информационной безопасности подчиняется руководителю своего соответствующего подразделения ИКТ, со всеми преимуществами и ограничениями, которые такая схема предполагает.

Международный вычислительный центр Организации Объединенных Наций как ключевой поставщик услуг кибербезопасности для системы

Международный вычислительный центр Организации Объединенных Наций в течение ряда лет предоставляет услуги по кибербезопасности примерно двум третям организаций системы Организации Объединенных Наций, хотя клиентская база каждой из его 13 связанных с этим услуг существенно различается. В этом разделе его каталога услуг наблюдается значительный рост по разным направлениям, при том, что на него по-прежнему приходится лишь небольшая часть бюджетных расходов Центра. Согласно отзывам участвующих организаций, они по-разному оценивали услуги кибербезопасности Международного вычислительного центра Организации Объединенных Наций, при этом «Общая аналитика угроз безопасности» была признана ее флагманской услугой. Еще в 2019 году ОИГ предлагала эффективнее использовать нереализованный потенциал Центра, особенно его услуги кибербезопасности. Организациям системы Организации Объединенных Наций и Центру рекомендуется найти больше точек соприкосновения, чтобы в возросших масштабах дополнить имеющиеся внутренние возможности организаций общими услугами. В этом духе исполнительным главам участвующих организаций предлагается пересмотреть нынешние договоренности организаций и вновь рассмотреть возможности использования предоставляемых Центром услуг кибербезопасности. Деятельность Международного вычислительного центра

Организации Объединенных Наций как межучрежденческой структуры, функционирующей в соответствии с правилами и в рамках административной структуры Всемирной организации здравоохранения, основана на модели самоокупаемости и совместного обслуживания. Эта модель как содействовала, так и препятствовала превращению Центра в узел кибербезопасности всей системы. В результате возникла ситуация, в которой предложение услуг Международного вычислительного центра Организации Объединенных Наций зависит от предоставления клиентами авансового начального финансирования затрат на разработку новой услуги для удовлетворения спроса, в то время как многие могут позволить себе приобретение разработанной таким образом услуги только после того, как на нее уже подпишется критическая масса клиентов. Учитывая проблемы, связанные с кибербезопасностью, и риски, с которыми сталкиваются организации, было сочтено своевременным изучить возможность использования добровольных взносов в качестве дополнительного механизма финансирования для прямого привлечения в больших объемах ресурсов для обеспечения кибербезопасности в рамках всей системы. Инспекторы считают, что создание в дополнение к существующим механизмам финансирования целевого фонда добровольных взносов, выделяемых для совместных решений в области кибербезопасности в рамках всей системы, может способствовать устранению некоторых имеющихся здесь препятствий. Целевой фонд не только позволит заинтересованным государствам-членам вносить свой непосредственный вклад в повышение кибербезопасности во всей системе, но и даст возможность улучшить с помощью механизма управления фондом, созданного соответствующими заинтересованными сторонами, связи между стратегическим руководством, которое может обеспечить Специальная группа по информационной безопасности, и функциональными возможностями, имеющимися у Международного вычислительного центра Организации Объединенных Наций (рекомендация 3). Генеральной Ассамблее предлагается принять к сведению эту рекомендацию и предложить донорам делать взносы в целевой фонд (рекомендация 4).

Цель более тесного согласования соображений физической безопасности и кибербезопасности

Хорошо известно, что Департамент охраны и безопасности имеет общесистемный мандат на выработку стратегии и руководство функциональными механизмами физической защиты и безопасности во всех организациях по всему миру. Несмотря на сближение между физическим пространством и киберпространством, когда речь идет о защите персонала и имущества организации, мандат Департамента охраны и безопасности, данный Генеральной Ассамблеей, касается конкретных угроз безопасности, относящихся к его компетенции, и поэтому не содержит каких-либо конкретных упоминаний кибербезопасности или киберизмерения рисков и угроз. Необходимость более тесного согласования между физической безопасностью и кибербезопасностью, очевидно, в течение ряда лет служит основой дискуссий в нескольких межучрежденческих органах, которые, однако, еще не привели к принятию практических выводов для системы. Чтобы помочь прояснению возможностей и рисков, связанных с распространением на киберсферу преобладающего подхода, основанного на оценке рисков, и структурированного, ориентированного на подотчетность реагирования, лежащих в основе Системы обеспечения безопасности Организации Объединенных Наций, инспекторы рекомендуют Генеральному секретарю представить Генеральной Ассамблее доклад, в котором следует рельефно выделить возможности более комплексной защиты персонала и ресурсов Организации Объединенных Наций и указать необходимые меры по соответствующему укреплению существующих структур, уделяя особое внимание роли Департамента охраны и безопасности в этом вопросе. Доклад должен быть основан на результатах консультаций между соответствующими межучрежденческими координационными механизмами, которые занимаются кибербезопасностью, и Межучрежденческой сетью по обеспечению безопасности, при необходимости, с участием Международного вычислительного центра Организации Объединенных Наций (рекомендация 5).

Рекомендации

Рекомендация 1

Исполнительным главам организаций системы Организации Объединенных Наций следует в первоочередном порядке и не позднее 2022 года подготовить всеобъемлющий доклад о своей системе кибербезопасности и представить его своим соответствующим директивным и руководящим органам при первой возможности, охватив элементы, способствующие повышению киберустойчивости, рассмотренной в настоящем докладе.

Рекомендация 2

Директивным и руководящим органам организаций системы Организации Объединенных Наций следует по мере необходимости рассматривать доклады об элементах, способствующих повышению киберустойчивости, подготовленные исполнительными главами, и давать стратегические указания относительно дальнейших улучшений, которые должны быть достигнуты в их организациях.

Рекомендация 3

Директору Международного вычислительного центра Организации Объединенных Наций следует стремиться к созданию не позднее конца 2022 года целевого фонда донорских взносов, который дополнил бы возможности Центра по проектированию, разработке и предложению общих услуг и решений для улучшения состояния кибербезопасности в организациях системы Организации Объединенных Наций.

Рекомендация 4

Генеральной Ассамблее Организации Объединенных Наций следует не позднее чем на своей семьдесят седьмой сессии принять к сведению рекомендацию, адресованную директору Международного вычислительного центра Организации Объединенных Наций, о создании целевого фонда для совместных решений по кибербезопасности и предложить государствам-членам, желающим улучшить состояние кибербезопасности в организациях системы Организации Объединенных Наций, сделать взносы в целевой фонд.

Рекомендация 5

Генеральному секретарю следует представить Генеральной Ассамблее Организации Объединенных Наций не позднее ее семьдесят восьмой сессии доклад об изучении дальнейших возможностей использования сближения физической безопасности и кибербезопасности в целях обеспечения более комплексной защиты персонала и ресурсов Организации Объединенных Наций, определяющий необходимые меры по соответствующему укреплению имеющихся структур, с уделением особого внимания возможной роли Департамента охраны и безопасности в этой связи.

Эти официальные рекомендации дополняются 35 неофициальными или нестрогими рекомендациями, выделенными жирным шрифтом в тексте настоящего доклада, в качестве дополнительных предложений, которые, по мнению инспекторов, могли бы улучшить состояние кибербезопасности в системе Организации Объединенных Наций.

Содержание

Приложения

Акронимы и сокращения

БАПОР	Ближневосточное агентство Организации Объединенных Наций для помощи палестинским беженцам и организации работ
ВМО	Всемирная метеорологическая организация
ВОЗ	Всемирная организация здравоохранения
ВОИС	Всемирная организация интеллектуальной собственности
ВПП	Всемирная продовольственная программа
ВПС	Всемирный почтовый союз
ИКАО	Международная организация гражданской авиации
ИКТ	информационно-коммуникационные технологии
ИМО	Международная морская организация
ИСО	Международная организация по стандартизации
КСР	Координационный совет руководителей системы Организации Объединенных Наций
МАГАТЭ	Международное агентство по атомной энергии
МОТ	Международная организация труда
МСЭ	Международный союз электросвязи
МТЦ	Международной торговый центр
НПО	неправительственная организация
ОИГ	Объединенная инспекционная группа
ООН-женщины	Структура Организации Объединенных Наций по вопросам гендерного равенства и расширения прав и возможностей женщин
ПРООН	Программа развития Организации Объединенных Наций
Теневая ИТ	теневая информационная технология
УВКБ	Управление Верховного комиссара Организации Объединенных Наций по делам беженцев
УНП	Управление Организации Объединенных Наций по наркотикам и преступности
ФАО	Продовольственная и сельскохозяйственная организация Объединенных Наций
Хабитат ООН	Программа Организации Объединенных Наций по населенным пунктам
ЮНВТО	Всемирная туристская организация
ЮНЕП	Программа ООН по окружающей среде
ЮНЕСКО	Организация Организации Объединенных Наций по вопросам образования, науки и культуры
ЮНИДО	Организация Объединенных Наций по промышленному развитию
ЮНИСЕФ	Детский фонд Организации Объединенных Наций
ЮНКТАД	Конференция Организации Объединенных Наций по торговле и развитию

ЮНОПС	Управление Организации Объединенных Наций по обслуживанию проектов
ЮНФПА	Фонд Организации Объединенных Наций в области народонаселения
ЮНЭЙДС	Объединенная программа Организации Объединенных Наций по ВИЧ/СПИДу

I. Введение

A. Контекст

1. **Важность кибербезопасности в цифровую эпоху.** В современном цифровом мире кибербезопасность стала важным вопросом для международных организаций, и организации системы Организации Объединенных Наций не являются исключением. Цифровая трансформация, растущая зависимость от информационно-коммуникационных технологий (ИКТ) и кибер-решений, а также тот факт, что угрозы для кибербезопасности постоянно растут, как по изощренности, так и по разрушительному потенциалу, привели к беспрецедентному увеличению рисков для кибербезопасности, с которыми сталкиваются Организации системы Организации Объединенных Наций. Инциденты, которые когда-то считались экстраординарными, становятся все более частыми и обычными. Инспекторы напоминают письмо, адресованное Генеральному секретарю в 2017 году, в котором представители комитетов по надзору системы Организации Объединенных Наций, собравшиеся на свое организованное впервые совещание, в числе трех основных проблем, вызывающих озабоченность у организаций системы Организации Объединенных Наций назвали необходимость того, чтобы руководство уделяло должное внимание новым и возникающим рискам, в частности глобальным и критическим для деятельности организаций угрозам, возникающих для кибербезопасности, а также рискам, появляющимся в результате новых способов работы по мере ускорения цифровой трансформации[1]. В этой связи организации — участницы Объединенной инспекционной группы (ОИГ) поддержали изучение ОИГ правил и практики кибербезопасности, имеющихся в системе Организации Объединенных Наций, которое было проведено ОИГ в рамках ее программы работы на 2020 год, став последним из серии обзоров на технологическую тематику по таким вопросам, как управление ИКТ, ведение интернет-сайтов и использование услуг облачных вычислений[2].

2. **Система Организации Объединенных Наций как объект кибератак.** Ландшафт угроз кибербезопасности в котором действуют организации системы Организации Объединенных Наций, не отличается от ландшафта угроз для других структур в том смысле, что инициаторы, средства и цели атак — от финансовых до символических — одни и те же. Различие, если оно и есть, может заключаться в том, что Организация Объединенных Наций может считаться предпочтительной целью по сравнению с другими организациями частного и государственного сектора. Во-первых, такая предпочтительность может заключаться в высокой заметности и глобальном масштабе деятельности структур Организации Объединенных Наций, что делает их более заметной мишенью для хакеров, желающих прославиться, по сравнению с известностью, которую можно получить, совершая атаки на какую-либо одну государственную организацию или структуру государственного сектора. Кроме того, в отличие от многих целей в частном секторе, они также могут быть более привлекательными для «хактивистов», которые руководствуются идеологическими мотивами и протестуют или выступают против ценностей, которые отстаивают или пропагандируют организации системы Организации Объединенных Наций. В силу межправительственного характера деятельности таких организаций имеется также неоспоримый политический элемент, на который сами организации только намекают, но, без исключения, который они признают само собой разумеющимся. В общем, хотя методы атаки идентичны, мотивы могут быть разными. Ясно то, что за последние пять лет наблюдается экспоненциальный рост числа атак, мелких и масштабных, на организации — участницы ОИГ, о чем свидетельствуют данные, полученные инспекторами из различных источников.

[1] Письмо на имя Генерального секретаря от 26 января 2017 года.
[2] JIU/REP/2008/5; JIU/REP/2008/6; JIU/REP/2011/9 и JIU/REP/2019/5.

3. **Выход киберинцидентов за рамки нарушения работы системы и их возможное влияние на выполнение мандата.** Для организаций системы Организации Объединенных Наций потенциальные последствия слабости системы кибербезопасности выходят за рамки нарушения возможностей административной обработки, инфраструктуры и систем ИКТ, и не должны оцениваться только по объему информации и данных, которые в конечном итоге оказываются скомпрометированы. Даже один случай несанкционированного доступа может иметь катастрофические последствия для организации, если происходит утечка конфиденциальных данных, таких как личная информация, истории болезни сотрудников, данные, составляющие интеллектуальную собственность, исторические и политические архивы и т. п. Кроме того, на карту поставлена способность организаций выполнять свои мандаты, а также их авторитет перед своими государствами-членами и партнерами. В сфере деятельности этих организаций даже незначительные технические сбои могут вызвать эффект домино, который может помешать дипломатическим и межправительственным процессам, гуманитарным мероприятиям или, в худшем случае, даже международному миру и безопасности. Хотя кибератаки могут по-разному влиять на организации системы Организации Объединенных Наций с разными мандатами и структурой, их угроза реальна для всех[3]. Ни одна организация не может ожидать, что никогда не столкнется с киберинцидентом, вне зависимости от степени ее готовности и бдительности. Однако игнорирование рисков может иметь значительные репутационные, практические, юридические и финансовые последствия.

4. **Признание важности кибербезопасности международным сообществом и Организацией Объединенных Наций.** Понимание того, что враждебная деятельность в киберпространстве составляет угрозу как для международного сообщества, так и, конкретно, для организаций системы Организации Объединенных Наций, получило документальное отражение в резолюциях и докладах соответствующих директивных и руководящих органов и механизмов внутренней координации, по крайней мере, с начала 1990-х годов. Предметные дискуссии по этому вопросу идут по параллельным направлениям. С одной стороны, они ведутся государствами как членами директивных и руководящих органов Организации Объединенных Наций, разрабатывающих глобальные меры реагирования на появление киберпреступности и киберугроз («обращенный вовне» аспект работы Организации Объединенных Наций в области кибербезопасности, в отношении которого компетенция общесистемной координации принадлежит Комитету высокого уровня по программам Координационного совета руководителей системы Организации Объединенных Наций — КСР), и, с другой стороны, организациями системы Организации Объединенных Наций, стремящимися усилить, как коллективно, так и самостоятельно, свою внутреннюю организационную готовность и меры реагирования на связанные с этим проблемы («обращенный вовнутрь» аспект, входящий в компетенцию Комитета высокого уровня по вопросам управления). Признание двуединой роли системы Организации Объединенных Наций в этом вопросе подтверждается заключительными словами выступления Генерального секретаря, которое он сделал в рамках КСР не так давно, в 2019 году: «Системе Организации Объединенных Наций необходимо взять на себя ведущую роль и выработать единую позицию в отношении кибербезопасности и угроз в этой области, одновременно служа платформой для обсуждения государствами-членами и другими заинтересованными сторонами вопросов кибербезопасности в ее различных аспектах»[4].

5. **Ответственность государств за защиту имущества Организации Объединенных Наций включает цифровые ресурсы в киберпространстве.** Что касается правовой защиты кибербезопасности, то организации системы Организации

[3] Общие сведения о проблемах, с которыми сталкиваются организации системы Организации Объединенных Наций, см. брошюру «Цифровые голубые каски Организации Объединенных Наций», опубликованную Управлением информационно-коммуникационных технологий Организации Объединенных Наций.

[4] CEB/2019/2, para. 39.

Объединенных Наций привлекают привилегии и иммунитеты, которые распространяются на их имущество, ресурсы, архивы, документы и переписку в широком смысле[5]. Предоставление таких привилегий и иммунитетов налагает на государства-участники обязательство в соответствии с их соответствующим законодательством обеспечивать защиту и безопасность, необходимую для достижения целей организации, обладающей такими привилегиями и иммунитетами, и обеспечить, в частности, неприкосновенность помещений, архивов и документов, «где бы они ни находились». Иными словами, государства и, в частности, принимающие страны обязаны ограждать организации от враждебных атак, будь то в физической или цифровой сфере. Это толкование было подтверждено инспекторам Управлением по правовым вопросам и разрешает вопрос о том, подпадают ли электронные данные и цифровые ресурсы под действие существующих правовых норм. Фактически, в более поздних соглашениях о штаб-квартире и с принимающей страной, заключенных на двусторонней основе между организациями и государствами, принимающими их на своей территории, Управление по правовым вопросам указывало, что термин «архивы» был прямо определен как включающий электронную почту и компьютерные данные, а также любые подобные материалы, принадлежащие данной организации или хранящиеся у нее для выполнения ею своих функций. Считается, что защищенная связь также включает электронную передачу данных, тогда как другие соглашения более широко предусматривают неприкосновенность любых используемых средств связи. В самом широком смысле это означает, что государства несут ответственность по международному праву за защиту ресурсов Организации Объединенных Наций, в том числе в киберпространстве.

6. **Эволюция от ИКТ к более широкой перспективе.** Традиционно вопросы кибербезопасности сначала возникали и решались в сфере ИКТ, игравших на заре компьютерных технологий менее заметную роль в деятельности организаций, чем сегодня. Это понимание кибербезопасности как дисциплины, ориентированной на ИКТ, было логическим следствием того времени, когда угрозы в основном ограничивались вычислительной инфраструктурой и затрагивали гораздо более узкий круг информационных ресурсов и организационных процессов. Однако теперь, когда ИКТ прочно вошли в практику большинства видов деятельности организаций, а ландшафт угроз значительно расширился за пределы простых технических сбоев, требующих более простых решений и технологических средств защиты, уже не представляется возможным рассматривать кибербезопасность только через ограничительную призму одних ИКТ. **Наоборот, инспекторы считают, что кибербезопасность должна определяться гораздо более широким взглядом на вещи, охватывающим несколько организационных областей и компетенций, включая управление рисками организации, физическую защиту и безопасность, защиту и конфиденциальность данных, юридическое обеспечение и информационную безопасность в более широком контексте управления информацией и знаниями.**

7. **Планирование бесперебойности деятельности как ключ к основанному на оценке рисков подходу к кибербезопасности.** Некоторые организации уже начали применять концепцию планирования повышения устойчивости деятельности организации, одним из многих аспектов которой является кибербезопасность. Основная задача этой области организационной устойчивости — адекватная оценка киберрисков с целью принятия превентивных мер, мер по снижению рисков и защиты от угроз, с одной стороны, и внедрение адекватных протоколов для руководства действиями и сохранения бесперебойности деятельности в случае материализации таких рисков — с другой. Снижение рисков в области кибербезопасности, которое никогда не бывает абсолютным, является скорее вопросом степени, и его

[5] Статья 105 Устава Организации Объединенных Наций; Конвенция о привилегиях и иммунитетах Объединенных Наций от 13 февраля 1946 года; Конвенция о привилегиях и иммунитетах специализированных учреждений от 21 ноября 1947 года; Соглашение о привилегиях и иммунитетах Международного агентства по атомной энергии от 17 августа 1959 года.

эффективность должна оцениваться не только по его успеху в предотвращении угроз, но и по степени, в которой он может помочь восстановить деятельность, нарушенную в результате атаки. Поэтому при возникновении серьезных инцидентов важно иметь хорошо отлаженную процедуру аварийного восстановления всех имеющихся информационных систем. Этого можно добиться только в том случае, если протоколы восстановления будут регулярно и тщательно тестироваться в рамках обычного планирования бесперебойности деятельности, в идеале с использованием тестирования на проникновение в качестве мощного инструмента контроля рисков. Хотя процедуры аварийного восстановления имеют большую техническую составляющую, для того чтобы они были эффективными, они должны разрабатываться в рамках стратегических параметров, установленных руководством организации (включая допустимые пределы риска, имеющиеся ресурсы и т. п.), и имеющихся эксплуатационных ограничений (таких, как приемлемое время восстановления). Соответственно, планирование бесперебойности деятельности, наряду с контролем рисков, становится неотъемлемой частью планирования устойчивости деятельности организации как для физических угроз, так и для киберугроз[6].

B. Цели, сфера охвата и методика

Цели

8. Проведение настоящего обзора преследует следующие основные цели:

a) выявить и проанализировать общие проблемы и риски кибербезопасности, с которыми сталкиваются организации системы Организации Объединенных Наций, и их соответствующие меры реагирования на них, принимая во внимание соответствующие сходства и различия в конкретных требованиях организаций и возможностях ограждения ими своих основных ресурсов при сохранении возможностей выполнения своих мандатов; а также

b) изучить ныне действующие межучрежденческие договоренности и их отдачу в плане содействия общесистемному подходу к кибербезопасности, а также выявить возможности улучшения координации, взаимодействия и обмена информацией между организациями системы Организации Объединенных Наций, где это необходимо.

Сфера охвата

9. **Общесистемный охват.** Настоящий обзор проводился на общесистемной основе и охватывал все участвующие организации ОИГ, а именно Секретариат Организации Объединенных Наций, его департаменты и управления, фонды и программы Организации Объединенных Наций, другие органы и подразделения Организации Объединенных Наций, специализированные учреждения Организации Объединенных Наций и Международное агентство по атомной энергии (МАГАТЭ). Международный торговый центр (МТЦ) не принимал участия в процессе обзора и поэтому не представлен в итоговых цифрах, показанных в настоящем докладе. Кроме того, ОИГ изучила деятельность Международного вычислительного центра Организации Объединенных Наций, учитывая его роль в предоставлении услуг кибербезопасности нескольким организациям системы Организации Объединенных Наций.

10. **Основное внимание к механизмам внутренней кибербезопасности.** В настоящем докладе основное внимание уделяется внутренним механизмам, созданным для управления системами кибербезопасности в организациях системы Организации Объединенных Наций, которые предназначены для защиты их ресурсов в киберпространстве и обеспечения реализации предусмотренной в их мандатах

[6] Программа работы ОИГ на 2021 год включает обзор, специально посвященный бесперебойности деятельности.

деятельности («обращенный вовнутрь» аспект кибербезопасности)[7]. Межправительственная работа системы Организации Объединенных Наций по содействию государствам-членам, в том числе в виде технической помощи в создании национального потенциала кибербезопасности или борьбе с киберпреступностью, представлена в приложении I для общего сведения, но не является предметом настоящего обзора. В приложении содержится краткий ретроспективный анализ рассмотрения этого вопроса в рамках различных направлений работы Генеральной Ассамблеи и других межправительственных органов.

11. **Технические аспекты подробно не анализируются.** Хотя кибербезопасность не является чисто технической проблемой, ее нельзя решать без учета ее аспекта ИКТ. Однако инспекторы не пытались глубоко проанализировать меры, принимаемые организациями, в плане их технологической адекватности или надежности. Для изучения технических соображений, потребовавшегося для полноты настоящего доклада, инспекторы привлекли внешних экспертов и ограничились выделением отдельных областей для рассмотрения и возможного дальнейшего изучения. В частности, они не претендуют на то, чтобы дать в настоящем докладе всесторонний сопоставительный или иной анализ степени развития каждой организации системы Организации Объединенных Наций. Считалось, что такой анализ выходит за рамки доклада, а также имеет ограниченную полезность для заинтересованных организаций, как по отдельности, так и вместе взятых.

12. **Связанные области обработки данных, которые имеют отношение к кибербезопасности, но выходят за рамки доклада.** Различные области управления знаниями и информацией, а также области защиты данных, конфиденциальности и связанные с ними области пересекаются с кибербезопасностью, но выходят за рамки настоящего исследования. Некоторые из них уже были рассмотрены в докладах ОИГ (например, информация как подтема документоведения и архивоведения)[8], в то время как другие затрагиваются на уровне отдельных организаций на основе общесистемных рекомендаций (например, отражение Принципов защиты персональных данных и конфиденциальности, принятых КСР в 2018 году, в правилах и административных инструкциях организации). Кроме того, проблемы и сложности, связанные с введением в том же году Общего положения о защите данных Европейского совета и попытками обеспечить его соблюдение в отношении организаций системы Организации Объединенных Наций, представляют собой отдельную группу вопросов, которые затрагивают кибербезопасность, но выходят за рамки настоящего исследования. Эти вопросы, не составляя исчерпывающий перечень, иллюстрируют широкий охват кибербезопасности как сквозной области, которую в настоящем докладе можно затронуть лишь бегло. **Однако инспекторы хотели бы отметить, что, в частности, область защиты данных и конфиденциальности личной информации является вопросом, имеющим большую актуальность и интерес, и что специальный критический анализ политики и практики организаций системы Организации Объединенных Наций в этом плане был бы своевременным и необходимым.**

Методика

13. В соответствии с внутренними стандартами и процедурами работы ОИГ для обеспечения согласованности, достоверности и надежности своих выводов инспекторы использовали ряд методов сбора качественных и количественных данных из различных источников. Информация, использованная при подготовке настоящего доклада, актуальна по состоянию на май 2021 года.

- **Анкеты и кабинетное изучение.** ОИГ собрала информацию с помощью двух анкет, разосланных участвующим организациям. Инспекторы изучили

[7] Настоящий доклад дополняется письмом, адресованным исполнительным главам участвующих организаций ОИГ и посвященным рискам, связанным с сохранностью и защитой юридических, нормативных, административных, политических и исторических документов и данных (JIU/ML/2021/1).

[8] JIU/REP/2013/2.

соответствующие элементы применимой нормативно-правовой базы (резолюции руководящих органов, организационные стратегии ИКТ, а также конкретные директивы и процедурные руководства по информационной безопасности и кибербезопасности, если они имеются) и ознакомились с докладами внутренних и внешних надзорных органов. Несколько запросов в Международный вычислительный центр Организации Объединенных Наций позволили провести критический анализ его мандата, каталога услуг и институционального, а также функционального потенциала в области кибербезопасности. Управление по правовым вопросам представило письменные разъяснения по ряду правовых аспектов. Анализ докладов комитетов и сетей КСР, главным образом Сети по цифровизации и технологиям и ее Специальной группы по информационной безопасности, помог получить более полное представление о межучрежденческой динамике и нынешних и прошлых общесистемных инициативах. Инспекторы также ознакомились с соответствующими отраслевыми стандартами и литературой по кибербезопасности в качестве справочной документации.

- **Беседы.** На основе заполненных анкет инспекторы провели 45 бесед с сотрудниками, отвечающими за ИКТ, и в частности кибербезопасность, а также со старшими должностными лицами, чтобы ознакомиться с более широкой организационной перспективой. Последующие беседы были проведены с представителями надзорных органов, Департамента охраны и безопасности, а также отдельных неучаствующих организаций. Беседы с председателем Специальной группы по информационной безопасности и представителями секретариата КСР позволили получить более полное представление о межучрежденческих инициативах по кибербезопасности. Беседы с представителями Международного вычислительного центра Организации Объединенных Наций дали подробную информацию о возможностях обеспечения кибербезопасности силами Центра. Инспекторы также присутствовали на Конференции по общей кибербезопасности 2020 года, организованной Международным вычислительным центром Организации Объединенных Наций и проведенную в виртуальном формате из-за продолжавшейся пандемии коронавирусной инфекции (COVID-19), чтобы получить представление о текущих событиях и проблемах, обсуждаемых подписчиками этой услуги Международного вычислительного центра Организации Объединенных Наций. Кроме того, с помощью фокус-группы инспекторы ознакомились с мнениями и опытом нескольких главных сотрудников по информационной безопасности как членов неформальной всемирной сети городских властей, сталкивающихся с аналогичными проблемами, благодаря чему они узнали о правилах, практике и опыте этих городских властей, которые могли бы послужить примером регулирования в государственном секторе для структур Организации Объединенных Наций.

14. **Ограничения в плане доступности и конфиденциальности информации.** Инспекторы столкнулись с ограничениями, в основном связанными со следующими моментами: a) доступность информации (поскольку статистика киберинцидентов не регистрировалась систематическим образом или, когда такая систематическая статистика имелась, не соответствовала общепринятой методике, что также ограничивало сопоставимость данных); b) конфиденциальность данных об угрозах, инцидентах и, в частности, о мерах реагирования, поскольку организации считали, что обмен такой информацией создает ненужный риск, связанный с выявлением и раскрытием уязвимостей их инфраструктуре безопасности, поэтому информация была представлена в первую очередь в сводной форме в описательной части доклада, без указания конкретных организаций, если только это не было необходимо в каждом конкретном случае; и c) влияние пандемии COVID-19 на процесс сбора данных, приводившее к задержкам и необходимости проведения собеседований только по видеосвязи, что могло сказаться на возможности общения с некоторым собеседникам, а также на их готовности делиться конфиденциальной информацией, которая в другом случае могла бы быть получена при личном общении. Кроме того, хотя инспекторы стремились изучить и отразить конкретное влияние мер реагирования участвующих

организаций на пандемию на соображения кибербезопасности, некоторые механизмы и меры, реализованные в этом контексте, могли получить дальнейшее развитие и, таким образом, не могли быть полностью отражены в процессе обзора.

15. **Слово признательности.** Инспекторы хотели бы выразить признательность всем сотрудникам организаций системы Организации Объединенных Наций и представителям других организаций, которые оказали помощь в подготовке настоящего доклада, в частности тем, кто участвовал собеседованиях и со столь большой готовностью поделились своими знаниями и опытом. В целях обеспечения качества был использован метод внутренней коллегиальной проверки для получения комментариев от инспекторов ОИГ по проекту доклада, который впоследствии был направлен заинтересованным организациям для представления теми своих комментариев по результатам, выводам и рекомендациям, а также для исправления любых фактических ошибок.

16. **Рекомендации.** Настоящий доклад содержит пять официальных рекомендаций, одна из которых адресована Генеральной Ассамблее, одна — директивным и руководящим органам, одна — исполнительным главам организаций — участниц ОИГ, одна — Генеральному секретарю и одна — директору Международного вычислительного центра Организации Объединенных Наций. Для облегчения работы с настоящим докладом и выполнения его рекомендаций и его контроля в приложении X содержится таблица, в которой указывается, был ли доклад представлен соответствующим организациям для принятия мер или для информации, а также требуют ли рекомендации действий со стороны директивных и руководящих органов или исполнительных глав организаций. Официальные рекомендации дополняются 35 неофициальными рекомендациями, выделенными жирным шрифтом, в качестве дополнительных предложений, которые, по мнению инспекторов, могли бы улучшить состояние кибербезопасности в системе Организации Объединенных Наций.

C. Определения

17. **Отсутствие общепринятого определения кибербезопасности.** Международные и национальные отраслевые стандарты информационной безопасности часто содержат определение кибербезопасности. Однако не существует общепринятого определения или глобального консенсуса относительно того, что именно подразумевается под этим термином. Инспекторы отметили, что в Организации Объединенных Наций не только не было каких-либо общесистемных разъяснений со стороны соответствующих межучрежденческих форумов, которые бы единогласно рекомендовали конкретное определение как авторитетное для системы[9], но и организациями также не было предпринято систематических попыток введения определения кибербезопасности в своей нормативно-правовой базе. В настоящем докладе инспекторы решили использовать определение кибербезопасности, разработанное Международным союзом электросвязи (МСЭ), которое воспроизводится во вставке 1. Подавляющее большинство участвующих организаций ОИГ подтвердили, что это определение отражает их подход к вопросу, часто дополняемый использованием ими как основы соответствующих отраслевых стандартов.

[9] Общесистемная концепция кибербезопасности и киберпреступности Организации Объединенных Наций (см. CEB/2013/2) и план внутренней координации по кибербезопасности и киберпреступности системы Организации Объединенных Наций (2014 год, приложение) содержат определения для выработки общего понимания терминов «киберпреступность» и «кибербезопасность» с той оговоркой, что это функциональные рабочие определения, не одобренные как таковые системой Организации Объединенных Наций.

Вставка 1
Кибербезопасность согласно определению Международного союза электросвязи

«Кибербезопасность — это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды и ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее: доступность; целостность, которая может включать аутентичность и неотказуемость; конфиденциальность».

Рекомендация Международного союза электросвязи (МСЭ) МСЭ-Т X.1205, Обзор кибербезопасности.

18. **Информационная безопасность и кибербезопасность.** Многие организации используют термин «информационная безопасность», который обозначает безопасность информации во всех ее формах и на любых носителях, а не только электронных данных в цифровой сфере. Кибербезопасность, напротив, может быть больше связана с защитой только цифровой информации и более широкого круга ресурсов, связанных с киберпространством или затронутых им, как видно из определения МСЭ. Несмотря на небольшие концептуальные расхождения между обоими терминами, они в значительной степени перекрываются, особенно в том, что касается основных целей защиты доступности, целостности и конфиденциальности информации (также известных как «триада информационной безопасности», как показано на диаграмме I). Некоторые организации используют термин «кибербезопасность» как синоним термина «информационная безопасность». Другие считают, что термин «кибербезопасность» заменил более традиционный термин «информационная безопасность», хотя и с потерей некоторых его более широких значений и коннотаций, связанных с информационными системами, в пользу свойств, скорее характеризующих ИКТ; есть и те, кто использует термин «кибербезопасность» как общий термин, включающий как «информационную безопасность», так и более узкий (и реже используемый) термин «безопасность ИКТ», который конкретно относится к безопасности инфраструктуры ИКТ (например, оборудования, программного обеспечения, сетей и технических процессов).

Диаграмма I
Модель триады информационной безопасности[10]

Источник: Национальный институт стандартов и технологий Соединенных Штатов Америки.

19. Сходная терминологическая двусмысленность наблюдалась в номенклатуре, относящейся к руководящим функциям, в рамках которых кибербезопасность, как правило, помещалась в организационный контекст. Например, «главный сотрудник по информационной безопасности» может подчиняться «главному сотруднику по информационным технологиям» или «главному сотруднику по информации», где последние два названия используются как синонимы для обозначения должности начальника отдела ИКТ или главного сотрудника по информационным технологиям. Не представляется возможным выявить закономерность, которая предполагала бы концептуальную осмысленность или строгость в определении различий в объеме функций, связанных с каждым термином.

20. В докладе инспекторы используют термин «кибербезопасность», как тот определен выше. Всякий раз, когда упоминается «информационная безопасность», этот термин употребляется намеренно для точного отражения исходных документов при прямом цитировании или правильного использования технических терминов, таких как «главный специалист по информационной безопасности» или «Система обеспечения информационной безопасности». Тем не менее инспекторы пришли к выводу, что в его пересмотре или в унификации его использования нет необходимости, поскольку он не препятствует передаче соответствующей информации и обмену ей между организациями.

[10] Согласно определению Центра интернет-безопасности, триада конфиденциальность–целостность–доступность — это эталонная модель в области информационной безопасности, предназначенная для регулирования и оценки того, как организация обращается с данными при их хранении, передаче или обработке. Каждый элемент триады представляет собой критически важную составляющую информационной безопасности, как показано ниже. Конфиденциальность означает, что доступ к данным или их считывание невозможны без санкции. Это гарантирует, что доступ имеют только стороны, которым он разрешен. Попытки нарушить конфиденциальность данных — это попытки их разглашения. Целостность означает, что данные ни в коем случае не должны быть изменены или вскрыты. Предполагается, что данные остаются в должном виде и могут редактироваться только имеющими допуск сторонами. Попытки нарушить целостность преследуют цель изменения данных. Доступность означает, что данные должны быть доступны по разрешенному запросу. Это гарантирует, что, получив разрешение, стороны при необходимости будут иметь беспрепятственный доступ к данным. Попытки нарушить доступность преследуют цель уничтожения данных.

II. Краткая характеристика кибербезопасности в системе Организации Объединенных Наций

A. Растущее внимание к кибербезопасности при, однако, разной степени развития разных организаций системы

21. **Растущее осознание необходимости внимания к кибербезопасности.** В последние годы в организациях системы Организации Объединенных Наций растет, пусть и в разной степени, понимание того, что кибербезопасность требует внимания. Риск кибератак для организаций системы Организации Объединенных Наций и их привлекательность в качестве мишени для них неоспоримы, хотя и могут быть разными в зависимости от их мандата или внимания к ним общественности. Можно утверждать, что мандат или характер деятельности, а также информация, которой владеют или которой распоряжаются организации, повлияли на то, насколько быстро ими была воспринята важность кибербезопасности. Организации, работающие с политически щекотливыми данными, которые имеют последствия для международной безопасности или национальных или экономических интересов, а также организации, оперирующие большими объемами юридически деликатных данных, включая персональные данные наиболее уязвимых групп получателей содействия, похоже, раньше вступили на путь усиления защиты кибербезопасности, в то время как организации с относительно неконфликтными мандатами создавали систему киберзащиты более умеренными темпами. Кроме того, некоторые организации, которые оказались в центре внимания общественности из-за актуальности их мандатов, были вынуждены в короткие сроки значительно активизировать свои усилия (такие, как Всемирная организация здравоохранения (ВОЗ)), что касается и тех организаций, для которых масштабные или резонансные кибератаки усилили необходимость скорейших действий и укрепления их киберустойчивости (такие, как Международная организация гражданской авиации (ИКАО)). В целом, однако, нет ни одной участвующей организации ОИГ, которая в той или иной форме не признала бы важность надежной кибербезопасности, определяемой условиями ее деятельности.

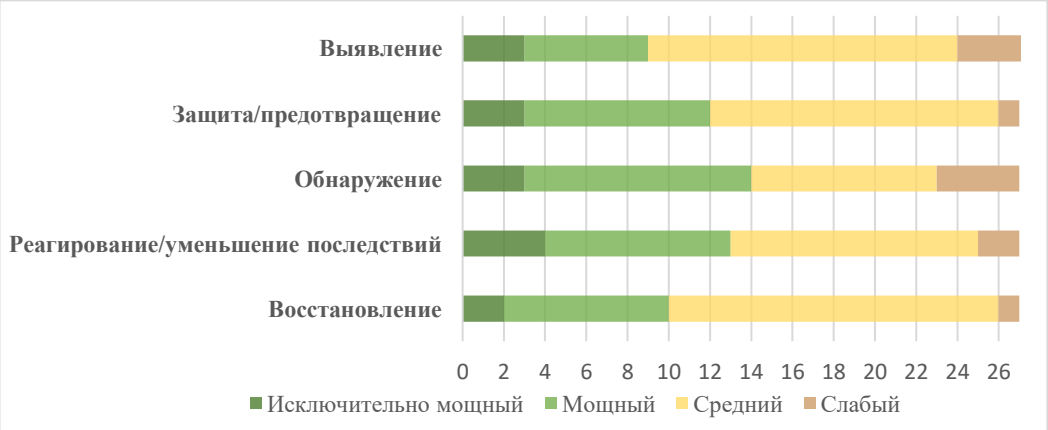
22. **Различия в степени развития между организациями системы Организации Объединенных Наций.** Хотя, было установлено, что ни одна из организаций — участниц ОИГ не забывала о необходимости вкладывать средства в свою кибербезопасность, наблюдались значительные различия в подходах различных организаций в ответ на киберугрозы: степень развития систем кибербезопасности организаций системы Организации Объединенных Наций значительно различается даже при отсутствии общих или единообразных критериев, которые могли бы облегчить методологически надежное, предметное сравнение. Эти различия могут объясняться следующим: условиями, в которых действует каждая организация; требованиями, продиктованными характером хранимых данных; уровнем понимания и приоритетом, определяемым для кибербезопасности их руководством; наличием ресурсов; а также большим разнообразием ИКТ-систем, инструментов и программных решений, используемых в масштабах системы, часто отражающим годы нескоординированных инвестиционных решений и выбора поставщиков в рамках всей системы. Несмотря на структурные и другие общие черты, которые, несомненно, присутствуют во многих, если не во всех организациях, изученных ОИГ, попытки дать окончательную оценку общей степени развития кибербезопасности системы Организации Объединенных Наций в целом не смогли бы должным образом отразить разнообразие, которым характеризуется ее состав. Кроме того, считается, что такая оценка имела бы ограниченную практическую ценность, поскольку сравнение с другими организациями или общесистемная «средняя» степень развития мало что говорили бы о защите данной организации.

23. **Полученные ответы предполагают, что имеются возможности для улучшений.** В попытке дать приблизительное представление о статус-кво на диаграмме II показано, как участвующие организации оценивали свою общую систему кибербезопасности по широким категориям функциональных областей, определенных в вопроснике ОИГ. При всех очевидных проблемах с интерпретацией полученных

ответов в отсутствие общей эталонной системы или образца для сравнения, общая картина, тем не менее, не дает оснований считать, что во всей системе в целом состояние кибербезопасности не вызывает беспокойства, даже с субъективной точки зрения. Международный вычислительный центр Организации Объединенных Наций в своей оценке общей системы кибербезопасности в организациях системы Организации Объединенных Наций, отвечая на тот же вопрос, и в той степени, в которой он мог дать представление о своей клиентуре, оценивал ее от «средней» до «слабой», что еще раз подтверждает, что имеются возможности для улучшений на общесистемном уровне.

Диаграмма II

Оценка состояния кибербезопасности в ее широких областях с разбивкой по категории мер защиты и числу организаций — участниц Объединенной инспекционной группы



Источник: Вопросник ОИГ 2020 года.

Примечание: Категории для самооценки в концептуальном плане основывались на типологии, использованной в авторитетных системах и стандартах в области кибербезопасности. Области кибербезопасности, упомянутые в вопроснике ОИГ, выделены следующим образом: выявление (критические процессы, активы, ресурсы, риски и т. п.); защита/предотвращение (управление доступом, осведомленность, обучение, процедуры, технологии и т. п.); обнаружение (аномалии и события, постоянный мониторинг, процесс обнаружения и т. п.); реагирование/уменьшение последствий (планирование, связь, анализ, уменьшение последствий и т. п.) восстановление (планирование, восстановление, связь, улучшения и т. п.).

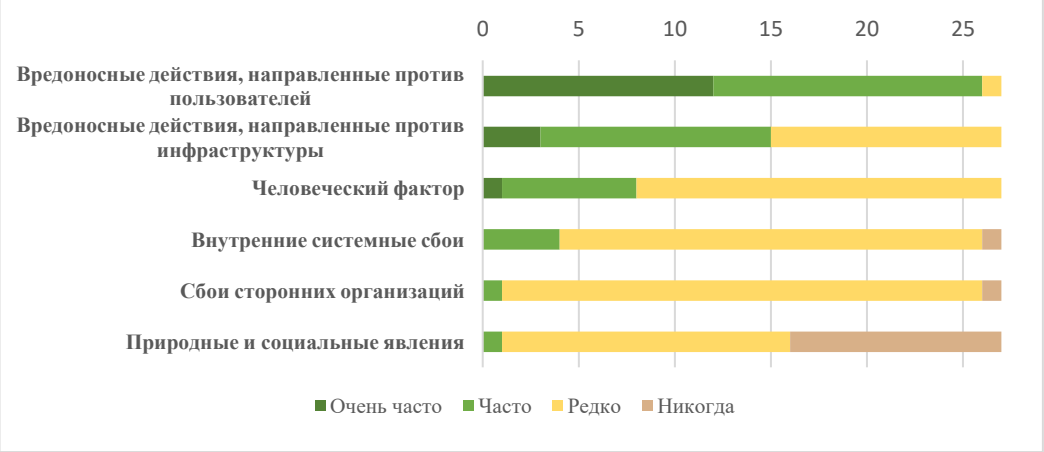
24. **Усиление общесистемных рисков из-за слабого состояния кибербезопасности в отдельных организациях.** Вопрос об адекватном уровне готовности к киберинцидентам выходит за рамки уязвимости отдельных организаций в этой области. В ходе бесед эксперты по кибербезопасности подтвердили мнение о том, что организация с уязвимой или слабой защитой представляет риск для других организаций системы. Как только злоумышленник получает права администратора и более глубокий доступ к информационным системам одной организации, такой доступ может быть использован для проникновения на цифровую территорию другой организации. Злонамеренное перемещение от одной организации к другой (известное как «проброс») также может быть труднее обнаружить и пресечь, поскольку оно может выглядеть как обычный трафик. Получив информацию об инфраструктуре одной организации, хакеры могут дополнительно скорректировать метод атаки и задействовать для достижения своей цели специально подобранный набор приемов и средств. Таким образом, организации, считающие свою систему кибербезопасности «слабой», создают проблему для всех из них. Таким образом, можно сказать, что система Организации Объединенных Наций не прочнее ее самого слабого звена. Этот аспект более подробно рассматривается в главе IV настоящего доклада.

B. Ландшафт угроз кибербезопасности

25. **Наиболее распространенные источники угроз и средства нарушения защиты.** Резюмируя нынешнюю подверженность киберугрозам, диаграмма III отражает ответы, полученные от участвующих организаций ОИГ в отношении эпизодичности инцидентов, с которыми они столкнулись за последние пять лет, с разбивкой по источникам угроз. Вредоносные действия, направленные против пользователей информационных систем (такие как фишинг, кража личных данных, перехват канала связи и т. п.) или инфраструктуры (вредоносное ПО, распределенные атаки «отказ в обслуживании» и т. п.), были, безусловно, наиболее распространенными категориями угроз. Сотрудники, с которыми были проведены беседы, подтвердили, что в недавнем прошлом наиболее распространенную и быстрорастущую категорию атак составляли злонамеренные действия, затрагивающие конечных пользователей. Эта ситуация усилилась в условиях пандемии, которая вынудила многих конечных пользователей работать из удаленных мест, часто с использованием личного оборудования, которое во многих случаях и в той или иной степени создает дополнительную нагрузку на меры защиты кибербезопасности организации (пп. 39–41).

Диаграмма III

Подверженность киберугрозам за последние пять лет с разбивкой по категории источников угроз и числу организаций — участниц Объединенной инспекционной группы



Источник: Вопросник ОИГ 2020 года.

Примечание: Источники угрозы далее описывались следующим образом: вредоносные действия, направленные против пользователей информационных систем (такие, как фишинг, кража личных данных, перехват канала связи и т. п.); вредоносные действия, направленные против инфраструктуры (вредоносный код, распределенные атаки типа «отказ в обслуживании», другие технические действия и т. п.); ошибка конфигурирования, нарушение правил эксплуатации, несоблюдение протокола, потеря оборудования и т. п. внутренний сбой системы (сбой устройства или системы или аппаратный сбой, отключение питания, неисправность линии связи и т. п.); сторонние сбои (интернет-провайдеры, электросеть, удаленное управление устройствами и т. п.); природные и социальные явления (наводнения, землетрясения, взрывы, массовые беспорядки, пожары и т. п.).

26. **Усиление атак с применением методов социальной инженерии, в частности во время пандемии COVID-19.** Хотя угрозы кибербезопасности обычно связаны с технически сложным воздействием на инфраструктуру, специалисты по кибербезопасности Организации Объединенных Наций сообщили о заметном переходе от хакерских атак на серверы, сети и конечные устройства, к злонамеренному воздействию на людей с помощью методов социальной инженерии, направленных на манипулирование людьми для получения конфиденциальной информации в мошеннических целях. Пандемия COVID-19 усугубила риски, связанные с социальной инженерией. Более двух третей участвующих организаций сообщили о резком усилении угроз и уязвимостей кибербезопасности во время глобальных

ограничительных мер, которые лишили многих пользователей доступа к централизованным ресурсами кибербезопасности, когда обращение к специально подготовленным специалистам для получения рекомендаций по подозрительным электронным письмам и веб-сайтам усложнилось из-за внезапного перехода к удаленной работе. Как сообщил Международный вычислительный центр Организации Объединенных Наций, киберпреступники и злоумышленники также воспользовались путаницей и возросшим интересом к материалам, связанным с пандемией, разослав фишинговые электронные письма на тему COVID-19 и создав фальшивые сайты с вредоносным кодом, якобы предоставляющие информацию о болезни. Фишинговые атаки были особенно успешными в это время, которое также было отмечено беспрецедентными масштабами распространения дезинформации, иногда с целью эксплуатации.

27. **Конкретные проблемы, связанные с методами социальной инженерии.** В отличие от атак на инфраструктуру, непосредственно нацеленных на ограниченное число вычислительных ресурсов, которые может быть проще защитить, защита от социальной инженерии считается в нескольких отношениях сложной задачей. Хотя они технически просты, такие атаки призваны одновременно охватить многих пользователей, что увеличивает вероятность несанкционированного доступа. Кроме того, хотя атакам с привлечением социальной инженерии подвергаются конечные пользователи, те часто являются лишь точкой входа, через которую открывается путь к другим важным ресурсам. Несанкционированный доступ, которому неосознанно способствуют сотрудники, может оставаться незамеченными в течение многих лет, предоставляя злоумышленникам широкий доступ к внутренней архитектуре безопасности и конфиденциальной информации, что, в свою очередь, открывает дополнительные возможности для атак. Это может включать проброс трафика, используемый для перемещения из киберсреды одной организации в киберсреду другой после первоначального получения доступа к локальным ресурсам, объединенным общей или связанной инфраструктурой. Этот прием вызывает особую озабоченность у организаций системы Организации Объединенных Наций, многие из которых имеют общие помещения, центры обработки данных или серверы, поскольку из-за него даже самые современные и надежные системы защиты организаций становятся столь же уязвимыми, как и самое слабое звено в их цепи. Поэтому особенно важно обеспечить надлежащее обучение и информированность всей группы пользователей, чтобы усилить надежность способов защиты.

28. **Прочие угрозы.** Организации также назвали человеческий фактор немаловажным источником уязвимостей, связанных с ошибками конфигурирования, нарушением правил эксплуатации, несоблюдением протокола, потерей оборудования или непреднамеренным повреждением по незнанию в более широком смысле. Сообщается, что сбои сторонних организаций случаются редко, что обнадеживает, указывая на то, что организации, по всей видимости, проявляют достаточную осмотрительность при выборе своих коммерческих партнеров. Стихийные бедствия, а также другие опасности, включая сбои, вызванные конфликтом или терактами, были, как сообщается, наименее распространенными, но они представляют собой важную область, где соображения физической безопасности и кибербезопасности должны идти рука об руку для уменьшения последствий.

29. **Происхождение угроз.** В условиях Организации Объединенных Наций, а также в целом киберинциденты могут исходить от широкого круга злоумышленников (вставка 2), которые могут быть внутренними или внешними по отношению к организации и могут действовать умышленно (преднамеренные атаки) или неумышленно

Вставка 2
Основные типы злоумышленников в киберсреде

- **Хакеры**. Лица или группы, которые взламывают сети, чтобы дезорганизовать, повредить или парализовать их, в основном ради известности или самоутверждения.

- **Хактивисты**. Хакеры с определенными мотивами, которые рассматривают свою деятельность как форму гражданского неповиновения или как средство политического или идеологического самовыражения.
- **Киберпреступники**. Лица, которые участвуют в преступной деятельности с использованием информационных технологий (уголовных преступлениях, таких как мошенничество, кража, вымогательство и т. п., с помощью компьютеризированных средств) или в преступной деятельности в среде информационных технологий (например, распространение вирусов или вредоносных кодов и другие действия, которые могут быть совершены только в среде компьютеризированных средств). В зависимости от уровня технической подготовки и организационного потенциала участники такой деятельности могут быть разными, от небольших группировок до крупных организованных преступных сообществ.
- **Лица, занимающиеся промышленным шпионажем**. Злоумышленники этой категории, которых иногда выделяют в отдельную подкатегорию преступников, преследуют специфические цели — получение сведений, составляющих коммерческую тайну, шантаж с целью получения экономических выгод или причинение ущерба конкурентам — и чаще всего встречаются в корпоративном мире.
- **Государственные или действующие при поддержке государства группы**. Злоумышленники с серьезной квалификацией и хорошо обеспеченные ресурсами, чью деятельность, как правило, трудно обнаружить, отследить или идентифицировать, которые могут скрытно преследовать сложные, часто косвенные и неочевидные цели и непосредственно привлекаются или косвенно финансируются государственными властями или военными структурами. В прошлом государства в основном создавали потенциал проведения расследований, но в последние годы стало общепризнанным фактом, что некоторые из них приобрели еще и потенциал наступательных действий.
- **Инсайдеры**. Субъекты, которые в силу договорных отношений с данной организацией не считаются внешними, создавая угрозу для нее изнутри. К ним, в частности, могут относиться недовольные сотрудники, плохо обученный персонал или сторонние обслуживающие организации.

(непреднамеренные действия или бездействие, либо их использование без их ведома). Некоторые преступные группы предлагают свои возможности другим злоумышленникам за плату, своего рода подряд на кибератаки, что можно назвать «киберпреступление как услуга». Таким образом, на вопрос о том, кто стоит за конкретной атакой (определение источника угрозы), сложно ответить не в последнюю очередь из-за множества механизмов, призванных скрыть реальное происхождение атаки (например, с помощью спуфинга, ботоферм и т. п.). В этой связи ряд собеседников — должностных лиц признали, что организации системы Организации Объединенных Наций не только не имеют возможности надежно определить источник атаки, но и не проявляли желания установить, кто стоит за взломом сети, поскольку связанные с этим затраты намного перевешивают пользу или положительные результаты. Многие из них отметили, что они в первую очередь стремятся к предотвращению, обнаружению и реагированию на атаки, не расходуя время и ресурсы на преследование злоумышленников, поскольку для этого потребуются значительные усилия, и, даже если злоумышленники будут успешно остановлены, это не решит проблему, поскольку организации подвергнутся новым атакам. Это также справедливо для феномена целенаправленных многоходовых кибератак, которые, как подтвердили организации, происходят достаточно части и нередко принимают форму проникновения, слежения и программных закладок, требующих определенного уровня ресурсов и изощренности, обычно связываемых с атаками, проводимыми при помощи государств.

C. Известные и неизвестные последствия инцидентов, связанных с кибербезопасностью

30. **Сообщения об ограниченном воздействии.** Чтобы лучше понять, в какой степени риск перерос в киберинциденты, которые затронули участвующие организации, ОИГ просила их оценить влияние прошлых инцидентов по степени серьезности (от незначительной до серьезной) и категории последствий (финансовые, эксплуатационные, цифровые, политические или репутационные, материальные или физические, или связанные с нарушением работы). Что любопытно и, возможно, удивительно, в своих ответах участвующие организации сообщали, что последствия киберинцидентов, с которыми они столкнулись, было небольшими или незначительными, независимо от категории последствий. В то же время признается, что число и частота предотвращенных киберинцидентов значительны, порядка тысяч в месяц, и в последние годы растут в геометрической прогрессии. Это говорит о масштабе киберугроз, которым сегодня подвергаются организации и их инфраструктура. Тем не менее, на первый взгляд и учитывая относительное отсутствие систематического сбора данных такого рода, это, по-видимому, указывает на в целом относительно ограниченные последствия.

31. **Области, наиболее затронутые атаками.** Организации сообщили, что области, наиболее затронутые кибератаками (последствия которых оценивались как «умеренные» сравнительно большим, но все еще ограниченным числом организаций и как «значительные» одной-двумя организациями, при том что ни одна из них не считала их «серьезными»), — цифровая сфера (в основном утечки данных), а затем политический и репутационный ущерб (дезинформация, неблагоприятное внимание СМИ, неправомерное вмешательство в межправительственные процессы и т. п.). Даже с финансовой точки зрения прямой ущерб (например, мошенническое списание средств) ограничился небольшими суммами, что с некоторой осторожностью можно воспринимать как свидетельство эффективности мер контроля в этой области. Однако инспекторы хотели бы обратить внимание на другие финансовые последствия кибератак (например, рабочее время и затраты, связанные с расследованием произошедшего и определением степени причиненного ущерба, затраты на восстановление ресурсов или оборудования, гонорары консультантов, привлекаемых для устранения последствий взлома, прекращение работы во время неработоспособного состояния системы или затраты на инвестиции для предотвращения будущих проблем), которые, возможно, с гораздо большим трудом поддаются количественной оценке, но, несомненно, значительны. В целом, несмотря на то что большинство участвующих организаций оценили свой потенциал реагирования в области кибербезопасности как «средний» (только треть сочла его «мощным» или «исключительно мощным»), влияние киберинцидентов, с которыми сегодня сталкивается Организация Объединенных Наций, как сообщается, само по себе не дает оснований для беспокойства.

32. **Неизвестная реальность.** Тем не менее несколько факторов позволяют считать приоритетное внимание к кибербезопасности оправданным. Во-первых, собранные данные оставляют некоторые белые пятна, подтверждая, что точные масштабы угрозы и ее последствий неизвестны, что было признано несколькими организациями в своих ответах. Чаще всего, особенно в случае более изощренных атак, злоумышленникам невыгодно раскрывать свое присутствие или использованные ими уязвимости, поэтому число проникновений в систему и утечек данных, вероятно, гораздо больше, чем сообщается. В этой связи несколько собеседников отметили, что доля «известных неизвестных» по сравнению с тем, что было известно о масштабах угрозы кибербезопасности, велика, но доля «неизвестных неизвестных» может вызывать еще большее беспокойство. Во-вторых, ответные меры могут (намеренно или непреднамеренно) занижать последствия, поскольку в корпоративной культуре, построенной на отчетности за результат и остром чувстве зависимости от ресурсов, связанных с такой отчетностью, честное признание слабых сторон еще не стало нормой как часть культуры организаций. Соответственно, это может исказить результаты. Например, в своих ответах на анкету ОИГ 11 участвующих организаций официально подтвердили, что в недавнем прошлом они подверглись по крайней мере

одной серьезной кибератаке, имевшей последствия для их деятельности. Однако есть организации, которые подверглись таким атакам, о чем стало общеизвестно, но не раскрыли этого в своих контактах с ОИГ. Таким образом, можно предположить, что реальная угроза, а также ее влияние превышают как то, что известно, так и то, что организации могут быть готовы раскрыть.

33. **Прошлые угрозы не позволяют судить о возможности новых инцидентов.** Несмотря на сказанное выше, эксперты пришли к единому мнению, что оценка серьезности угрозы по степени ее материализации в прошлом была бы ошибочной. Возможность ущерба остается высокой, и ее следует предвидеть, подготовив меры противодействия. Так, растущая угроза использования программ-вымогателей для вымогательства денег в обмен на украденные данные до сих пор, за некоторыми исключениями, по-видимому, обошла стороной организации системы Организации Объединенных Наций. Сообщения СМИ подтверждают, что несколько известных организаций, включая крупные компании частного сектора и даже органы местного самоуправления, были вынуждены заплатить выкуп, чтобы восстановить доступ к своим данным и информационным системам. Инспекторы отмечают, что в настоящее время участвующие организации занимают четкую позицию, исключая выплату какого-либо выкупа преступникам. В том же духе стоит отметить, что на данный момент организации системы Организации Объединенных Наций не сообщали о каких-либо кибератаках против подключенных устройств, таких как лифты, системы вентиляции, автономные транспортные средства или аналогичное оборудование с дистанционным управлением. Атаки на подключенные устройства — новая область угроз кибербезопасности, но организациям следует проявлять бдительность, поскольку эксперты в этой области прогнозируют значительный рост такого рода угроз в будущем. Эти два примера демонстрируют важность прогнозирования рисков, в отношении которых в системе Организации Объединенных Наций не имелось заметного числа прецедентов, и упреждающего учета соображений кибербезопасности в общем процессе управления рисками организаций.

34. **Киберстрахование.** Один из вариантов повышения упреждающей защиты от возникающих угроз — киберстрахование, позволяющее покрыть ущерб от кибератак, а также, возможно, избежать необходимости иметь дело с этическим аспектом вопроса о выплате выкупа. В каждом конкретном случае страховые компании по просьбе клиентов могут предоставить киберстрахование. В ходе работы над докладом ни одна из организаций системы Организации Объединенных Наций не сообщила, что она застраховала кибер-риски, хотя некоторые из них указали, что они рассматривали такую возможность. Признавая преобладающую позицию среди организаций системы Организации Объединенных Наций, инспекторы не считают киберстрахование эффективным инструментом упреждающего купирования соответствующих рисков в большинстве ситуаций их деятельности, особенно потому, что это была бы лишь стратегия частичного уменьшения последствий кибератаки, способствующая сведению к минимуму ее возможного финансового ущерба при небольшом выигрыше в плане уменьшения ущерба для деятельности или репутации. Тем не менее, **по мнению инспекторов, исполнительному руководству рекомендуется готовиться к возникновению таких угроз, которые могут усилиться в будущем.**

D. Взаимодействие и сотрудничество с национальными властями

35. **Неединообразная практика и ограниченное желание предоставлять данные национальным властям.** Участвующие организации придерживаются разной практики уведомления о нарушениях кибербезопасности национальных властей, которые могут иметь возможности расследовать и принимать административные или судебные меры в отношении кибератак. Около трети участвующих организаций сообщили, что они уведомляют об инцидентах национальные правоохранительные органы, но лишь немногие делали это систематически или регулярно. Среди организаций, которые сообщили, что в прошлом они взаимодействовали с национальными властями по вопросам кибербезопасности, большинство подтвердили, что такие уведомления направлялись на разовой основе, а

не в рамках установленного порядка или сложившейся практики организации. Многие использовали неформальные отношения на рабочем уровне, а не формальные каналы, где это возможно, и только в случае серьезных атак, которые предполагали либо вероятные последствия для принимающей страны, либо значительный репутационный риск для организации. Даже в тех случаях, когда возможности расследования на национальном уровне превышают и, таким образом, могут помочь дополнить внутренние — часто очень ограниченные — возможности преследования подозреваемых злоумышленников, немногие организации сообщили о желании или необходимости формализовать или расширить систематическое взаимодействие с национальными властями применительно к нарушениям кибербезопасности. Общая картина показывает, что готовность к взаимодействию с национальными властями ограничена и что предпочтение отдается поддержанию неформального взаимодействия «по мере необходимости».

36. **Факторы, влияющие на деятельность организаций.** Существуют различные факторы, из-за которых организации могут колебаться до обращения к национальным органам. Один из них — правовой статус организаций как обладателей привилегий и иммунитетов как таковых, особенно связанных с конфиденциальностью и неприкосновенностью их данных, которые должны быть ограждены от любого вмешательства законодательного, исполнительного или судебного характера. Границы юридических обязательств в этой сфере часто плохо понимаются специалистами по кибербезопасности. Фактически, хотя государства несут юридическое обязательство обеспечивать защиту, организации обязаны сотрудничать с национальными властями только в той степени, в которой такое сотрудничество не препятствует их способности независимо выполнять свои функции. Таким образом, такое сотрудничество всегда добровольно. Эта формула проводит тонкую грань, неочевидную на практике, но не должна из-за этого препятствовать добровольному взаимодействию, когда оно оправдано, и после всесторонней оценки его возможных рисков. В любом случае, нет обязанности сообщать об инцидентах национальным властям или разглашать какие-либо данные, которые считаются конфиденциальными. Решения по этому поводу лучше всего принимать по рекомендации юристов организации. Еще одним соображением при принятии решения об установлении контакта с национальными властями может быть степень развития аппарата кибербезопасности самой соответствующей страны, а также его действия по отношению к киберпреступникам, в отношении которых устанавливается национальная юрисдикция. Возможные здесь опасения тем более серьезны, когда к угрозе кибербезопасности организации причастны ее собственные сотрудники (случаи внутренних угроз). В таких случаях обычная процедура предусматривает отмену привилегий и иммунитетов и передачу данного лица государству его гражданства для дальнейшего расследования и возможного судебного преследования. Однако такое происходит сравнительно редко, в частности в случае кибернарушений. С 2007 года, когда начала собираться и публиковаться соответствующая статистика, только один случай неправомерного поведения персонала, который был передан через Управление по правовым вопросам национальным властям для дальнейшего расследования, был связан с нарушением информационной безопасности[11]. Помимо изложенных выше соображений, серьезность инцидента, полезность и вероятность установления того, кем именно была совершена атака, возможность необоснованного раскрытия конфиденциальной или закрытой информации и возможное влияние расследования на деятельность организации чаще всего упоминались в числе соображений, которые необходимо учитывать при принятии решения об обращении к национальным властям. Некоторые официальные лица также признали, что обращение к национальным властям часто даже не учитывается как вариант.

37. **Процесс принятия решений об уведомлении профильных национальных органов.** Как показано выше, решение о том, устанавливать ли контакт с национальными властями, затрагивает аспекты, выходящие за рамки компетенции экспертов по кибербезопасности. Речь идет о сочетании политических, юридических, доказательственных и практических соображений, поэтому такое решение должно

[11] A/75/217, приложение I.

приниматься с участием ряда заинтересованных сторон. В организациях, где инспекторы обнаружили признаки более устоявшегося подхода к взаимодействию с национальными властями, распределение обязанностей отражало спектр рассматриваемых соображений, что было сочтено полезным. Конкретно, затронутое программное или оперативное подразделение оценивает серьезность вторжения, взвесив программные риски и положительные стороны обращения к национальным властям. Юридическое подразделение оценивает и разъясняет возможные последствия правового характера с учетом особого статуса организаций и их сотрудников в соответствующих странах, включая возможную необходимость отмены привилегий и иммунитетов и, в соответствующих случаях, направление материалов на замешанного сотруднику стране его гражданства. Роль подразделения ИКТ или экспертов по кибербезопасности при этом заключается в предоставлении имеющихся данных, собранных в ходе расследования нарушения. Решение о том, поднимать ли далее этот вопрос перед принимающей страной, будет приниматься руководством при участии всех указанных выше заинтересованных сторон. После принятия решения о доведении инцидента до сведения национальных властей для этого обычно используются установленные каналы связи между соответствующими подразделениями организаций системы Организации Объединенных Наций, постоянным представительством соответствующего государства и компетентными властями принимающей страны. С учетом некоторых критических замечаний относительно эффективности налаженного процесса, можно было бы изучить некоторые альтернативные или дополнительные механизмы, некоторые из которых представлены в других разделах настоящего доклада (пп. 161–163).

E. Технологическая готовность — некоторые вопросы, требующие внимания

38. **Имеется хорошо развитый базовый технический потенциал, но следует обратить внимание на области, требующие более пристального внимания.** Инспекторы задали участвующим организациям ряд вопросов с целью изучения общего состояния их технической готовности к отражению киберугроз. При этом цель заключалась не в проведении всесторонней оценки надежности их рабочих механизмов или технической инфраструктуры, а в том, чтобы получить представление об общих имеющихся возможностях и выделить некоторые общие вопросы, которые заслуживают особого внимания. Принимая во внимание ограничения, присущие информации, собираемой в основном путем самооценки, а также значительные различия в степени детализации сведений, предоставленных инспекторам, из полученных ответов можно сделать вывод, что участвующие организации считают, что основные технические области кибербезопасности были хорошо изучены и получили большие вложения, соразмерные их соответствующим возможностям. Например, две трети участвующих организаций сообщили, что у них имеются средства текущего контроля сети. Кроме того, большинство организаций сообщают, что они создали системы сетевой защиты или другие системы защиты от несанкционированного доступа, в то время как 13 организаций сообщают о внедрении системы защиты сети и информационной безопасности. Именно в областях, в которых в последнее время происходило наиболее динамичное технологическое развитие, картина представляется более нюансированной и может потребовать некоторого внимания со стороны участвующих организаций. В этом разделе по соображениям безопасности созданные организациями системы подробно не рассматриваются, чтобы не дать оснований для выводов, которые могут поставить под угрозу защиту этих организаций.

Сопряжение оконечных устройств и средства организации удаленной работы

39. **Пандемия COVID-19 привлекла внимание к организации взаимодействия с оконечными устройствами.** Пандемия потребовала внедрения альтернативных и гибких систем взаимодействия в гораздо больших масштабах, чем ранее, почти для всех профессиональных групп, как в штаб-квартирах, так и на местах. На этом фоне способность организаций работать дистанционно в условиях ограниченного

физического доступа к помещениям и централизованного подключения компьютерного оборудования была подвергнута беспрецедентному испытанию на прочность, а инструменты, а средства организации удаленной работы стали предметом повышенного внимания в разрезе компьютерной безопасности. С одной стороны, это включает возможность сотрудников удаленно получать безопасный доступ к компьютерным ресурсам, и две трети организаций сообщили, что с этой целью они используют виртуальные частные сети, а остальные организации используют облачные сервисы с доступом по зашифрованным интернет-протоколам в общедоступной сети без необходимости использования виртуальных частных сетей. С другой стороны, для дистанционной работы необходимо сопряжение оконечных устройств (настольных и мобильных компьютеров, а также других мобильных устройств), применительно к которым организации указывают на разную степень совместимости.

40. **Отставание в организации взаимодействия с оконечными устройствами.** Хотя большинство организаций упоминают некоторую степень централизованного управления устройствами, некоторые из них, по-видимому, не обеспечивают полного взаимодействия. В некоторых случаях взаимодействие ограничивается оборудованием, находящимся только в штаб-квартире, при этом семь организаций отметили, что их отделения на местах используют другие системы организации взаимодействия с оконечными устройствами, а в других случаях с централизованной системой взаимодействуют только постоянно подключенные компьютеры, а около трети участвующих организаций вообще не обеспечивают ни организации взаимодействия с мобильными устройствами, ни их централизованной защиты, хотя в некоторых из них в настоящее время создаются или планируется в ближайшем будущем создать платформы такого рода. Только в двух ответах упоминается зашифрованное подключение оконечных устройств — современное решение для предотвращения кражи и утечки данных, особенно с портативных устройств конечных пользователей, которые обычно чаще теряются и похищаются. Ответы свидетельствуют о том, что организации осознают необходимость защиты подключения к своим сетям, но отстают в организации взаимодействия с мобильными устройствами. Существующие здесь уязвимости возросли из-за использования личных, а не служебных мобильных устройств, таких как личные ноутбуки, — получившего намного более широкое распространение во время пандемии.

41. **Принятие или ускорение реализации важных мер кибербезопасности.** Несмотря на множество возникших проблем, появление пандемии также вызвало некоторые положительные сдвиги. В силу безотлагательной необходимости подразделения Организации Объединенных Наций были вынуждены более внимательно изучить свои системы обеспечения безопасности и начали реализовываться запланированные организационные проекты ИКТ. Можно сказать, что массовый переход на удаленную работу в столь короткие сроки побудил многие организации активизировать свои усилия по повышению безопасности удаленного доступа и, судя по ответам на анкеты ОИГ, мог придать столь необходимый импульс активизации действий в этом направлении. В этой связи большинство организаций внедрили систему многофакторной аутентификации для удаленного доступа, в ранее беспрецедентных масштабах внедрили системы совместной работы и передачи данных в сети, дополнительно институционализировали использование электронных подписей и расширили возможности обучения по вопросам информационной безопасности. В известном смысле пандемия стала катализатором трансформации ИКТ в нескольких подразделениях Организации Объединенных Наций и подтолкнула их к цифровизации и внедрению передовых цифровых методов работы — фактор, имеющий последствия не только для области кибербезопасности, но и, в гораздо более широком смысле, для того, как организации строят свою работу, как и для того, как используются их ресурсы и помещения.

Системы прошлого поколения

42. **Конкретные уязвимости, создаваемые системами прошлого поколения.** Несколько участвующих организаций сообщили, что модернизация или выведение из эксплуатации действующих устаревших систем, которые могут больше не

поддерживаться современными приложениями, создает серьезные проблемы кибербезопасности. Было заявлено, что постоянное присутствие таких систем прошлого поколения представляет собой основной источник уязвимости, поскольку многие из них были разработаны для использования только локально, в частных — локальных или глобальных — сетях, которые считались безопасными. В основном из-за эволюции удаленного доступа и более широкого использования облачных вычислений эти приложения подвергаются теперь гораздо большему риску из-за возросшей взаимосвязанности систем и данных в более глобальном масштабе и при этом не созданы для защиты от более современных форм атаки. Некоторые из возникших в результате уязвимостей могут быть выявлены системами устранения уязвимостей, способными предупредить о них, но остается вероятность того, что некоторые коммерческие приложения прошлого поколения не будут выявлены автоматически. Даже при их выявлении они не всегда могут быть сразу же исправлены, что чревато чрезмерно длительным риском для этих организаций. Помимо рисков для самих приложений прошлого поколения, такие уязвимости также создают риск для других приложений и ресурсов, которые могут совместно использовать одну и ту же инфраструктуру, поскольку после их взлома приложения прошлого поколения могут использоваться для горизонтального перемещения между системами и приложениями.

43. **Необходимость тщательного анализа систем прошлого поколения.** Поэтому важно, чтобы организации системы Организации Объединенных Наций вели учет таких систем и активно работали над их обновлением или заменой. Поскольку некоторые из этих систем прошлого поколения являются большими и сложными (например, системы общеорганизационного планирования ресурсов) и многие из них создавались своими силами в течение длительных периодов времени, эта задача может быть сложна для многих, требуя дополнительных финансовых ресурсов и усилий для привлечения и поддержания заинтересованности подразделений, вложивших средства в разработку индивидуальных решений, которые теперь считаются небезопасными. **Инспекторы предлагают, чтобы исполнительные главы в тесном сотрудничестве с экспертами по ИКТ и кибербезопасности, а также с соответствующими подразделениями, начали тщательный анализ вопроса о системах прошлого поколения в своей организации, если они этого еще не сделали.** Важное место в таком анализе должны занимать соображения кибербезопасности, наряду со стратегическим и своевременным рассмотрением связанных с этим затрат, а также непосредственных и долгосрочных последствий вывода таких систем из эксплуатации для деятельности, которые следует устранять путем надлежащего планирования временных мер по уменьшению последствий, когда это возможно.

Безопасность облачной среды

44. **По мнению экспертного сообщества кибербезопасности защита, предлагаемая внешними поставщиками облачных услуг, значительно повысилась.** С 2019 года, когда ОИГ выпустила свой доклад об облачных вычислениях[12], как использование облачных услуг участвующими организациями, так и разнообразие и степень развития таких услуг значительно выросли. Их повсеместность, эластичность (способность постоянно оптимизировать распределение вычислительных ресурсов с учетом фактического спроса на ресурсы в реальном времени) и экономическая эффективность, а также их постоянное — растущее технологическое совершенство, внушили пользователям доверие к их надежности и безопасности, что еще больше повысило их привлекательность для системы Организации Объединенных Наций. Организации продолжают переносить свои существующие приложения на облачные сервисы, и решение об этом по-прежнему принимается каждой конкретной организацией. В этой связи инспекторы отмечают растущее признание сообществом экспертов по кибербезопасности того, что возможности облачных сервисов и гарантии, предлагаемые сегодня ведущими компаниями в этой области, превышают уровень безопасности данных, конфиденциальности и киберустойчивости, который они могли обеспечить всего

[12] JIU/REP/2019/5.

год-два назад. По мнению экспертов, защита, обеспечиваемая в настоящее время такими поставщиками услуг, также может превышать возможности любой отдельной организации по достижению сопоставимой степени безопасности с использованием решений собственной разработки. В ходе работы над настоящим докладом встретился только один пример того, когда участвующая организация решила полностью отказаться от облачных решений для работы с исключительно конфиденциальной частью своих данных. Однако стоит отметить, что этот выбор был сделан для ограниченного массива данных и определялся возможностями организации — включая финансовые — предложить жизнеспособную альтернативу, что не очевидно для большинства организаций.

45. **Необходимость постоянной бдительности при использовании внешних облачных сервисов.** Даже на фоне значительного прогресса, достигнутого в последние годы в области безопасности облачных решений, рекомендации исполнительным главам, содержащиеся в упомянутом докладе ОИГ, остаются в силе в отношении следующего: необходимость соответствия облачных решений производственным задачам для обеспечения отдачи затрат; всесторонняя оценка рисков и четкая работа с поставщиками при привлечении внешних поставщиков облачных услуг; стратегии снижения риска нарушения поставщиками контрактных обязательств о предоставлении услуг. Продолжают сохраняться также опасения относительно рисков монополизации и чрезмерной концентрации данных Организации Объединенных Наций в руках сравнительно небольшого числа технологических гигантов. Соответственно, организации не могут позволить себе ослабить бдительность при использовании облачных приложений или размещении своих приложений и данных в облачной среде, в частности с учетом риска несанкционированного доступа к конфиденциальным или закрытым данным. Они должны и далее проявлять должную осмотрительность и применять разумные методы кибербезопасности при использовании облачных услуг, в частности, требуя подтверждения соблюдения их поставщиками требований независимого аудита и предъявления соответствующих документов, таких как отчеты системного и организационного контроля, в частности «отчеты СОК-2», или аналогичные гарантии, широко признанные отраслевыми экспертами. Требование таких внешних независимых гарантий тем более важны, если учесть, что при привлечении внешних поставщиков на тех может не распространяться компетенция механизмов внутреннего аудита и других механизмов организационного надзора. Таким образом, при заключении контракта на такие услуги рекомендуется запрашивать мнение подразделения внутреннего аудита, чтобы обеспечить включение соответствующих положений, обеспечивающих разумную уверенность в соблюдении соответствующих стандартов внутреннего контроля в отношении сбора, хранения и использования размещенной информации. Также желательны консультации с юридическим подразделением. Поэтому организации должны найти приемлемые альтернативы для обеспечения степени контроля, которая считается адекватной, например, путем включения в договоры со сторонними поставщиками облачных услуг положений, позволяющих организации осуществлять надзор и контроль за соблюдением ее требований. Кроме того, коммерческие облачные ресурсы могут менять владельцев, даже перемещаться за границу, что в ряде случаев может еще больше усугубить риск раскрытия данных, размещенных или обрабатываемых на таких ресурсах, в случае попытки судебного разбирательства в соответствующем государстве. В таких ситуациях привилегии и иммунитеты будут заявляться и сохраняться в отношении всех данных, хранящихся по заданию организаций системы Организации Объединенных Наций. Однако организации должны сохранять бдительность и принимать необходимые меры предосторожности для максимального купирования таких рисков.

46. **Недостижимость нулевого риска и необходимость тщательного анализа.** При всех ожидаемых преимуществах в плане безопасности и экономической эффективности, инспекторы напоминают, что как облачные решения, так и традиционные подходы с использованием центров обработки данных подвержены киберугрозам и никогда не могут претендовать на полную защищенность. Поэтому нереально стремиться к полному устранению рисков в любой среде. Независимо от

того, передается ли риск в какой-то степени внешним структурам, которые выстраивают соответствующую вычислительную среду, ответственность за последствия кибератак остается внутри организации. Таким образом, организациям рекомендуется провести подробный анализ, прежде чем решать, готовы ли они доверить защиту своей информации третьим сторонам, и если да, то в каких аспектах. В этом плане оценки защиты данных должны гарантировать, что меры безопасности облачных решений соответствуют требованиям организаций и соразмерны характеру и уязвимости данных информационных ресурсов. Подобные соображения применимы к любому решению о передаче на сторону и поэтому не ограничиваются только ситуацией использования безопасности облачной среды.

Защита от уязвимостей

47. **Различия в практике участвующих организаций.** Защита от уязвимостей сегодня считается одной из главных проблем кибербезопасности в международных организациях. Почти ежедневно обнаруживаются новые уязвимости в широко используемом программном обеспечении, включая программное обеспечение (ПО), используемое организациями системы Организации Объединенных Наций. Хотя поставщики аппаратного и программного обеспечения постоянно разрабатывают и предоставляют соответствующие исправления, такие исправления выливаются в необходимость обработки существенного объема информации и значительной рабочей нагрузки, связанной с их внесением в технически сложных средах. Более половины участвующих организаций сообщили, что для решения этой проблемы они используют то или иное решение по защите от уязвимостей. Так, некоторые используют подписку на несколько информационных каналов, чтобы постоянно узнавать о новых угрозах (и защищаться от них), включая новые уязвимости, в то время как другие решили внедрить комплексные системы безопасности коммерческих поставщиков, включающие защиту от уязвимостей. Некоторые организации отмечали, что обнаружение и исправление уязвимостей — ответственное направление обеспечения кибербезопасности. Некоторые отметили, что злонамеренные попытки найти уязвимости в их сетях и системах со временем активизируются, в то время как распределенный характер их сети ИКТ затрудняет централизованное управление процессом исправления уязвимостей, в частности, в нескольких отделениях на местах. Несколько организаций также сообщили, что расходы на исправление уязвимостей входят в число наиболее значительных затрат, связанных с их программами кибербезопасности.

48. **Необходимо обеспечить постоянную защиту от уязвимостей.** Инспекторы обращают внимание на значительную разницу в эффективности между разовыми (например, ежегодными) оценками уязвимости и непрерывным процессом выявления и устранения уязвимостей. Если исправления не вносятся регулярно, системы ИКТ слишком долго остаются уязвимыми для средств злонамеренного использования уязвимости, и риск взлома значительно возрастает. Информация, полученная от участвующих организаций по этому вопросу, не позволяет с достаточной уверенностью считать, что эта проблема решается адекватным и последовательным образом. Ответы на анкету ОИГ от нескольких организаций скорее указывают на более эпизодическую оценку уязвимости (ежегодно или даже реже), в то время как другие организации, такие как Ближневосточное агентство Организации Объединенных Наций для помощи палестинским беженцам и организации работ (БАПОР), Всемирная продовольственная программа (ВПП), ИКАО и Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) считают эффективное и постоянное устранение уязвимостей полезной наработкой своих организаций. **В этой области есть возможности для улучшения, и инспекторы настоятельно призывают исполнительных глав уделять достаточное внимание и выделять адекватные ресурсы, позволяющие проводить регулярные оценки уязвимости для того, чтобы работа по защите от уязвимостей велась в организациях системы Организации Объединенных Наций на систематической основе.**

Теневые информационные технологии (теневые ИТ)

49. **Причины обращения к теневым ИТ.** Термин «теневые ИТ» относится к приложениям или решениям ИКТ, разработанным или принятым внутри организации, но за пределами ее официальной, обычно централизованной структуры ИКТ. Чаще всего теневая ИТ является результатом того, что пользователи пытаются решить практическую проблему с помощью инструментов, которые легко получить на рынке по низкой цене или бесплатно, когда решения, предоставляемые по установленным каналам и по линии подразделений ИКТ, могут считаться не отвечающими их требованиям по срокам, затратам или возможности настройки. Она также может быть результатом желания быстро вводить новшества в условиях изменения требований или обеспечивать согласованность или совместимость с инструментами, используемыми партнерами-исполнителями, которые могут не отличаться от решений, выбор которых утвержден в организации. Примеры этого — создание бесплатных учетных записей у поставщиков услуг, предлагающих решения по хранению данных, передаче файлов, веб-дизайну или управлению контентом, или разработка приложений своими силами для использования отдельными подразделениями, периферийными отделениями или проектами. Эти решения обычно не проверяются или не всегда проверяются на соответствие требованиям и процедурам кибербезопасности, установленным официальным централизованным органом на общеорганизационном уровне, и поэтому могут считаться работающими в несанкционированной, «теневой» среде.

50. **Риски, связанные с использованием теневых ИТ.** Сообщается, что это явление получило распространение в некоторых организациях, особенно в их отделениях на местах или подразделениях, которые иным образом дальше отстоят от централизованного контроля. В таких условиях риски часто усиливаются тем, что центральные подразделения ИКТ и кибербезопасности имеют ограниченное представление об используемых на местах ИКТ. И в этом случае пандемия COVID-19, внезапно потребовав удаленного выполнения многих функций, еще больше усугубила эту проблему, поскольку многие пользователи начали использовать средства сетевого взаимодействия, включая конференц-связь, помимо решений, включенных в используемые организациями пакеты программного обеспечения. Однако многие услуги, к которым пользователи обращались в качестве потенциальных альтернатив, не были изучены или одобрены для массового использования специалистами организаций по кибербезопасности, что может создавать риск для организаций (например, из-за того, что применяются не стандарты, которые рекомендованы на уровне организации в отношении аутентификации или конфиденциальности, а другие стандарты). Так, в самом начале пандемии Специальная группа по информационной безопасности изучила использование одной популярной онлайн-платформы видеоконференц-связи, чтобы оценить ее пригодность для использования организациями системы Организации Объединенных Наций, однако эксперты по кибербезопасности не смогли прийти к окончательному и однозначному решению — рекомендовать или не рекомендовать ее, — которое было бы действительным для всей системы. Вместо этого они изложили ряд вариантов, а также предостережений и мер предосторожности, которые следует учитывать при использовании этой онлайн-платформы в определенных условиях.

51. **Некоторые предложения по более тщательному контрою за теневым ИТ. Инспекторы считают, что проблемы кибербезопасности, связанные с использованием теневых ИТ, требуют большего внимания с уравновешиванием необходимости контроля в среде, подверженной киберрискам, и оправданными целями и конструктивной мотивацией пользователей к инновациям и использованию альтернативных решений при их наличии.** В этой связи имеются основания не считать сразу нежелательным стремление некоторых пользователей использовать теневые ИТ-решения, поскольку считается здоровым признаком готовности к инновациям, для которых подразделения, как правило, должны иметь определенные ресурсы и свободу действий, в идеале в безопасной и защищенной вычислительной среде. В этой связи могут быт восприняты, например, такие идеи: создание или расширение безопасных сред для цифровых инноваций; привлечение внимания к развитию распределенных ИКТ в более децентрализованных условиях с

привлечением местных координаторов ИКТ; а также активизация обучения конечных пользователей и мер по повышению осведомленности для получения надежной и четкой информации о безопасности и рисках использования сторонних сервисов вне стандартных процедур и практики и информации об утвержденных организацией альтернативах, а также рекомендаций о более безопасном использовании таких решений.

III. Элементы, способствующие повышению киберустойчивости

52. **Киберустойчивость как следствие культуры кибербезопасности.** Помимо технологической готовности, связанной с определением цифровых решений и источников данных для защиты организационных ресурсов, надежная кибербезопасность является результатом разностороннего подхода, охватывающего все уровни организации, включая директивные и руководящие органы, механизмы надзора, исполнительное руководство, оперативные или функциональные подразделения и руководителей программ, персонал в целом, а также партнеров-исполнители и внешних поставщиков услуг. Иными словами, для создания условий повышения киберустойчивости необходим общеорганизационный подход. Кроме того, кибербезопасность затрагивает несколько организационных областей и компетенций, включая ИКТ, управление рисками, физическую безопасность и защиту, а также управление информацией и знаниями в более широком смысле. Множество соображений и осведомленность всех заинтересованных сторон об их роли и вкладе в успешное поднятие планки кибербезопасности каждой организации можно считать составляющими культуры кибербезопасности, которая, укоренившись и войдя в практику, помогает организации достичь киберустойчивости. В настоящей главе инспекторы представляют свои выводы относительно того, в какой степени системы и практика участвующих организаций отражают такие элементы, которые способствуют повышению киберустойчивости (вертикальная перспектива), как показано на диаграмме IV, и предлагают возможные улучшения.

Диаграмма IV
Элементы, способствующие повышению киберустойчивости

Источник: Подготовлено ОИГ.

Примечание: В одном ведущем отраслевом стандарте киберустойчивость определяется как способность предвидеть, противостоять, восстанавливаться и адаптироваться к неблагоприятным условиям, стрессам, атакам или нарушениям в системах, которые используют киберресурсы или поддерживаются ими.

A. Взаимодействие с директивными и руководящими органами

Директивные и руководящие органы, обеспечивающие стратегическое руководство и ресурсы

53. **Кибербезопасность заслуживает внимания директивных и руководящих органов.** ОИГ постоянно заявляла, что директивные и руководящие органы межправительственных организаций должны играть решающую роль в обеспечении стратегического руководства и адекватных ресурсов для того, чтобы любая организация могла выполнять предусмотренную ее мандатом деятельность. Как указано в недавнем докладе ОИГ об общеорганизационном управлении рисками[13], директивным и руководящим органам следует проявлять заинтересованность и знать, как минимум, об основных стратегических рисках, с которыми сталкивается организация, и имеющихся стратегиях и механизмах управления ими. **По мнению инспекторов, это должно включать вовлеченность и руководство в области кибербезопасности, учитывая ее критический характер не только как вопроса управления рисками, но и как ключевого фактора, способствующего выполнению мандатов организаций.** Конкретные способы, с помощью которых соответствующие органы могут активнее участвовать и поддерживать общеорганизационные усилия в этой области, представлены во вставке 3. Однако, поскольку кибербезопасность по-прежнему воспринимается как преимущественно технический вопрос, степень привлечения директивных и руководящих органов к рассмотрению этой темы или ее вовлеченности в ее рассмотрение на сегодняшний день в большинстве организаций ограничена.

Вставка 3
Возможности вовлеченности директивных и руководящих органов в рассмотрение вопросов кибербезопасности

- Выработка четкой директивы в отношении допустимого риска для организации в вопросах кибербезопасности, прямо фиксирующей степень риска, который считается приемлемым в своем конкретном контексте. Имеется ограниченное число свидетельств существования таких директив в участвующих организациях, за исключением Программы развития Организации Объединенных Наций (ПРООН) и Всемирной организации интеллектуальной собственности (ВОИС), где создана современная и хорошо проработанная методика определения допустимой степени риска.
- Обеспечение стратегического руководства высокого уровня в приоритетных областях кибербезопасности. Хороший пример такого руководства — раздел «Информационная безопасность» стратегии Секретариата Организации Объединенных Наций в области информационно-коммуникационных технологий, которая была одобрена Генеральной Ассамблеей в 2014 году (A/69/517).
- Выделение адекватных финансовых ресурсов на основе проработанного обоснования, представленного исполнительным руководством, что позволит реализовать цели, изложенные в стратегических рекомендациях директивных и руководящих органов в соответствии с допустимой степенью риска.

54. **Практика вовлеченности директивных и руководящих органов.** Глубина и степень взаимодействия с директивными и руководящими органами в вопросах кибербезопасности различаются, в основном, в зависимости от мандата организации и практических соображений. Немногие организации осознают, не говоря уже о его использовании, потенциал активного взаимодействия с директивными и руководящими органами в вопросах кибербезопасности, а среди тех, которые осознают его, большинство пришли к этому только после того, как серьезная атака

[13] JIU/REP/2020/5.

потребовала повышенного внимания и взаимодействия на высшем уровне. Хотя формат такого взаимодействия может быть разным и не существует единого «правильного» уровня или степени взаимодействия, уже имеется определенное понимание того, что определенный информационный поток между лицами, отвечающими за кибербезопасность в организации, и ее членами не только полезен, но и, возможно, необходим. Ниже инспекторы проводят различие между механизмами регулярной отчетности о кибербезопасности и процедурами доведения инцидентов до сведения директивных и руководящих органов.

Механизмы отчетности и доведения до сведения вышестоящих руководителей

55. **Существующие механизмы отчетности.** Инспекторы обнаружили, что меньшинство организаций предусматривают ту или иную форму периодической отчетности по вопросам кибербезопасности для своих директивных и руководящих органов. Если такая отчетность предусмотрена, она представляется в разных формах: a) некоторые организации могут включать соответствующую информацию в свой программный бюджет и доклады о его исполнении (обычно в разделе ИКТ, который может прямо и не охватывать кибербезопасность); b) в других составляется специальная отчетность по запросу директивного и руководящего органа, например отчетность о ходе в реализации одобренных или принятых стратегий или дорожных карт; и c) третьи полагаются на ежегодную отчетность своих внутренних и внешних надзорных органов, используя ее в качестве основного канала для обоснования необходимости повышенного внимания к этой теме.

56. **Отсутствие систематического сбора и представления статистики кибербезопасности.** Также имеется несоответствие в содержании такой отчетности перед директивными и руководящими органами, при этом немногие организации делятся собираемой и анализируемой ими внутри нее статистикой по отдельным аспектам ее уязвимости и защищенности в области кибербезопасности. С одной стороны, такие несоответствия в практике отчетности могут быть результатом понятного нежелания многих организаций составлять общедоступную или даже закрытую статистику кибербезопасности, которая способна выявить уязвимости и тем самым повысить риски. С другой стороны, они могут отражать то, что организации все еще пытаются определить правильную степень детализации и наиболее актуальный набор показателей для отчетности, а также наиболее содержательную группу показателей, которые, собственно, необходимо составлять. Большинство участвующих организаций составляют показатели, характеризующие в основном эпизодичность, серьезность или масштабы киберинцидентов за определенный период времени, используя их для внутренних целей, при этом некоторым организациям еще предстоит закрепить или формализовать более разовые формы сбора данных. Однако характер собираемых и анализируемых данных существенно различается между организациями, а способы обработки таких данных сопровождения принятия решений, будь то внутри них или на уровне директивных и руководящих органов, во многих организациях еще не определены. Поскольку такие показатели служат одним из важнейших элементов, на основе которых можно определить допустимую для организации степень риска, **инспекторы считают целесообразным продолжить изучение различных наборов показателей кибербезопасности на соответствующих форумах и разработать базовую методику, которая при необходимости может быть адаптирована с учетом условий каждой организации**.

57. **Доведение киберинцидентов до сведения директивных и руководящих органов и преимущества прозрачности по отношению к ним.** Из ответов на вопросник ОИГ, представленных участвующими организациями, следует, что директивные и руководящие органы не информируются об инцидентах в области кибербезопасности систематическим образом. Кроме того, инспекторы обнаружили, что имеются ограниченные свидетельства того, что процессы доведения до сведения директивных и руководящих органов заранее определены на этот случай. Решение такого рода обычно принимается в каждом конкретном случае. Опыт тех организаций, которые имели возможность, часто вызванную крупными киберинцидентами, протестировать свои каналы выхода на руководящие органы, указывает на следующие основные факторы, которые следует учитывать при рассмотрении вопроса о

целесообразности доведения инцидента до сведения директивных органов: a) серьезность инцидента; b) влияние на деятельность организации; c) влияние на межправительственные процессы; и d) вероятность того, что инцидент станет достоянием общественности. Другие важные соображения — сроки доведения инцидента до сведения директивного органа и меры предосторожности, призванные не допустить раскрытия конкретных уязвимостей или подробных сведений о возможностях организации принимать ответные меры, способные привлечь новые атаки на нее. В ходе бесед эксперты по кибербезопасности обычно отмечали, что доводить инцидент до сведения директивного органа следует до того, как он будет полностью урегулирован, или, скорее, как только станет достаточно ясно, что происходит. Делать это сразу после обнаружения атаки может быть слишком рано и может поставить под угрозу предпринимаемые усилия по урегулированию, тем самым непреднамеренно увеличивая уязвимость. В то же время, если откладывать информирование директивного органа до полного урегулирования инцидента, то это может поставить под сомнение доверие к исполнительному руководству или его готовность обеспечивать прозрачность и принимать ответственность за возможные бреши в системе кибербезопасности. Общий настрой тех участвующих организаций, которые открыто сообщают своим директивным и руководящим органам об инцидентах и недостатках в их киберзащите, заключался в том, что не следует бояться обращения к ним, поскольку репутационные издержки, включая потерю доверия со стороны государств-доноров, намного перевешивают возможные последствия «потери лица» и ущерб, в том числе косвенные финансовые последствия, в результате атаки.

58. **Необходимо предусмотреть протоколы доведения киберинцидентов до сведения руководства как внутри организаций, так и для директивных и руководящих органов. По мнению инспекторов, важно заранее определить механизм, с помощью которого серьезные кибератаки будут доводиться до сведения директивных и руководящих органов.** Поскольку вероятность таких атак можно предвидеть, отсюда следует, что протокол доведения киберинцидентов до сведения руководства тоже может быть составлен заранее. В частности, критерии (в какой момент необходимо обращение к руководству) и механика того, кто должен предпринять какие именно шаги, в каком порядке и при чьем участии, не должны быть предметом реактивного принятия решений. Такое принятие решений, предполагающее импровизацию в момент острого кризиса, скорее всего, будет затрудняться необходимостью ситуативных антикризисных мер, в то время как соблюдение установленного протокола дало бы полную возможность заострить внимание на конкретных параметрах, неизбежно присутствующих в каждом конкретном случае. Кроме того, необходимость разработки таких мер в кризисном режиме сделает процесс более уязвимым для ненадлежащего влияния в и без того сложной и потенциально политизированной обстановке, чего можно в значительной степени избежать с помощью упреждающего подхода. Наконец, без ущерба для составленных внутри организаций протоколов о доведении инцидентов до сведения директивных и руководящих органов тем может быть целесообразно рассмотреть возможность обсуждения своего собственного порядка действий по таким вопросам в ожидании того, что серьезные случаи кибератаки будут переданы им для рассмотрения и принятия решения. Такой дальновидный подход может помочь установить некоторые тщательно продуманные и согласованные границы действий, предпринимаемых директивными и руководящими органами, и в свою очередь способствовать деполитизации и принятию взвешенных решений в этой потенциально чувствительной области.

B. Включение кибербезопасности в число контролируемых организациями факторов рисков

59. **Преимущества подхода к кибербезопасности, основанного на управлении рисками.** В недавнем докладе ОИГ общеорганизационное управление рисками охарактеризовано как общеорганизационный процесс структурированного, комплексного и систематического выявления, анализа, оценки, обработки и

мониторинга рисков для достижения целей организации[14]. Основные функции, связанные с кибербезопасностью (обычно варианты выявления, предотвращения, обнаружения, реагирования и восстановления), отражают ключевые этапы и цели управления рисками. Отношение к кибербезопасности как к проблеме управления рисками на общеорганизационном уровне также имеет конкретные практические преимущества. Во-первых, будучи признанной стратегической задачей всей организации, кибербезопасность становится вопросом, который касается всех подразделений и всех сотрудников, поощряя и поддерживая общеорганизационный подход и распределение функций по управлению рисками. **Кроме того, инспекторы подтверждают, что формальное включение кибербезопасности в концепцию общеорганизационного управления рисками способствует повышению важности этой темы среди разнообразных приоритетов организации и служит официальной отправной точкой, от которой директивные и руководящие органы и старшее руководство могут совместно вырабатывать план оптимального управления основными рисками.** Поскольку такие концепции, как правило, представляют собой живые документы, они также дают возможность систематического и периодического пересмотра, адаптации и индивидуализации мер по снижению рисков в свете быстро меняющихся требований организации.

60. **Парадигма управления рисками уже частично признана.** Полезность рассмотрения кибербезопасности через призму управления рисками уже была признана на различных форумах, хотя на практике последствия такого подхода к кибербезопасности во многих частях системы еще предстоит полностью понять и воспринять. Так, на недавних симпозиумах Специальной группы по информационной безопасности, на которых присутствовали эксперты по кибербезопасности, обсуждалось несколько пунктов повестки дня, касающихся управления рисками, в том числе призыв к ее членам взаимодействовать с представителями их соответствующих организаций, участвующими в работе Форума по управлению рисками Комитета высокого уровня по вопросам управления, чтобы обеспечить отражение рисков кибербезопасности в подходах, на основе которых Форум разрабатывает модель зрелости управления рисками[15]. Необходимость отражения соображений кибербезопасности в более общих концепциях общеорганизационного управления рисками и обеспечения бесперебойности деятельности также подчеркивалась комитетами по аудиту и надзору нескольких организаций. В этой связи большинство из них рассматривали кибербезопасность как часть своего мандата по общеорганизационному управлению рисками и подчеркивали необходимость большего сопряжения между функциями ИКТ и управления рисками. Кроме того, современные стандарты кибербезопасности, включая ИСО 27001, Цели контроля для информационных и связанных технологий и стандарты Национального института стандартов и технологий Соединенных Штатов, рассматривают риски кибербезопасности как организационные риски, далеко выходящие за пределы вычислительной инфраструктуры, и подчеркивают стратегический аспект улучшения состояния кибербезопасности в организациях, что считается достижимым наилучшим образом при полной корреляции с управлением рисками на организационном уровне.

61. **Внимание к управлению рисками в участвующих организациях.** Степень, в которой кибербезопасность рассматривается как проблема управления рисками, варьируется в зависимости от участвующих организаций, опрошенных ОИГ. В своих ответах подавляющее большинство (24 из 27) из них сообщили, что риски, связанные с кибербезопасностью, официально включены в их общеорганизационный реестр рисков. Из них 20 подтвердили, что присвоенный уровень риска был «высоким» (диаграмма V), а 19 включили конкретные меры по снижению рисков для кибербезопасности в свой общеорганизационный реестр рисков. Инспекторам была предоставлена внутренняя документация об управлении рисками только 11 участвующими организациями, которые предоставили в конфиденциальном порядке выдержки из своих реестров рисков. С учетом неполноты этих данных сделанные выводы следует считать предварительными. Однако, сравнивая некоторые

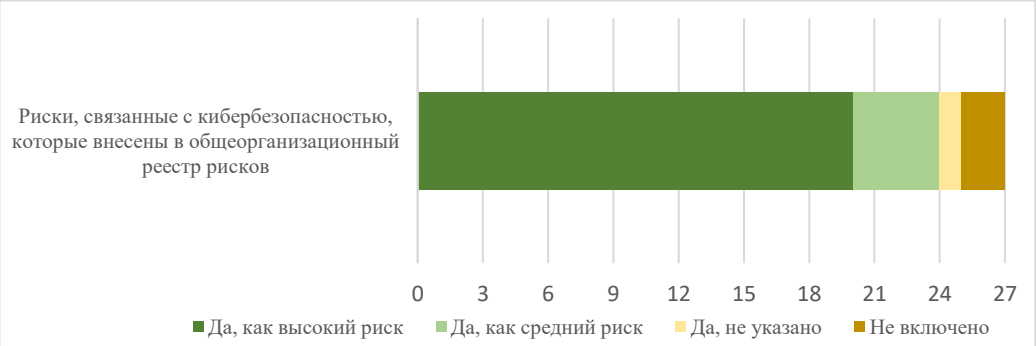
[14] JIU/REP/2020/5.

[15] CEB/2019/HLCM/DTN/02.

из представленных образцов реестра рисков, можно заметить определенные различия в оценке, классификации и планировании рисков для кибербезопасности. С одной стороны, некоторые организации сделали акцент на стратегических аспектах, таких как потенциальное влияние киберинцидентов на репутацию, деятельность и финансы организации. На другом конце спектра есть примеры реестров рисков, которые почти полностью сосредоточены на безопасности ИКТ, с основным упором на сохранении доступности информации, а не на ее конфиденциальности и целостности. Последнее, как правило, требует более сложных мер по сравнению с мерами, направленными только на предотвращение технических сбоев и «простоев», что может объяснить, почему эти аспекты в меньшей степени затрагивались в рассмотренной документации. Один из недостатков реестров рисков, в которых основное внимание уделяется главным образом техническим аспектам кибербезопасности, заключается в том, что они могут не устанавливать связи между этими элементами и более широкими последствиями для организации.

Диаграмма V

Число участвующих организаций, в которых риски для кибербезопасности включены в организационные реестры рисков



Источник: Вопросник ОИГ 2020 года.

62. **Необходимость большего внимания к мерам по уменьшению последствий.** Одна область, которая выделялась, даже при ограниченности данных, имевшихся у инспекторов, — это уровень разработки мер по снижению рисков кибербезопасности, либо как часть структуры управления рисками, либо вне ее. Как отметили комитеты по аудиту и надзору, меры по уменьшению последствий часто описывают статус-кво (например, подробно описывают уже принятые меры, а не предусматривают упреждающие действия в предвидении конкретных рисков), что приводит к замкнутому на себе процессу постановки уже достигнутых целей для улучшения отчетности, а не к серьезным усилиям по разработке результативных мер по уменьшению последствий в качестве критериев для постепенной реализации. Сознавая то, что некоторые организации, возможно, сознательно решили представить свои меры по уменьшению последствий в неконкретных терминах для ограждения мер защиты организации, **инспекторы считают, что в будущем упор следует делать на разработке мер по уменьшению последствий упреждающим образом, по-прежнему отражающим существующие ограничения и слабые места, признавая, что это может потребовать дополнительных усилий для достижения вновь установленных целей, а также переходного периода применительно к отчетности, которая может показать неполное достижение целей.**

63. **Дорожные карты.** В некоторых организациях оценка рисков кибербезопасности привела к принятию общеорганизационной дорожной карты по повышению киберустойчивости организации, подготовленной руководством с учетом отзывов всех соответствующих внутренних заинтересованных сторон и во многих случаях представленной на утверждение директивным или руководящим органам. Инспекторы считают, что такие дорожные карты имеют наибольший смысл тогда, когда они составляются как многолетний план, увязанный с контрольными точками и показателями достижений, сопровождаемый сдвигом в распределении ресурсов для

обеспечения практической реализации мер по уменьшению последствий. На момент составления настоящего доклада такие процессы разработки дорожной карты были завершены или продолжались в нескольких организациях (ИКАО, Продовольственная и сельскохозяйственная организация Объединенных Наций (ФАО), Фонд Организации Объединенных Наций в области народонаселения (ЮНФПА), Управление Верховного комиссара Организации Объединенных Наций по делам беженцев (УВКБ), Управление Организации Объединенных Наций по обслуживанию проектов (ЮНОПС) и Всемирная организация интеллектуальной собственности (ВОИС)) и считались полезными для оптимизации усилий по совершенствованию во всей организации.

64. **Переход от информированности к упреждающему управлению рисками.** Наконец, хотя многие участвующие организации осознали важность соображений кибербезопасности и попытались включить их с различной степенью четкости в свои более широкие концепции управления рисками, общесистемная картина по-прежнему неоднородна и требует дальнейшего внимания, чтобы перейти от простого осознания рисков для кибербезопасности к действительному управлению ими в соответствии с требованиями каждой организации при признании того, что в этой области нулевой риск недостижим. **Таким образом, инспекторы полностью соглашаются с настоятельным предостережением экспертов по кибербезопасности: ставки высоки, и требуется подход, основанный на оценке рисков (приложение II).** В будущем акцент должен быть сделан на разработке эффективных и результативных мер по снижению рисков в сочетании с надежным планированием бесперебойности деятельности. Решающее значение для достижения этих целей будет иметь вклад экспертов по кибербезопасности и их полное участие во внутренних процессах управления рисками, от разработки до внедрения и контроля.

C. Использование сближения физической безопасности и кибербезопасности

65. **Размытые границы между физической безопасностью и кибербезопасностью.** До известной степени философский вопрос о том, должна ли кибербезопасность рассматриваться как прежде всего «кибер»-проблема информационных технологий или проблема безопасности (сравнимая с физической защитой и безопасностью, но перенесенная в цифровую сферу) возник уже на раннем этапе, даже на этапе концептуализации настоящего обзора, и вызвал плодотворную дискуссию среди собеседников инспекторов. Хотя организации системы Организации Объединенных Наций традиционно рассматривают физическую безопасность и защиту и кибербезопасность как отдельные области, и та, и другая связаны с защитой персонала организаций и сохранением их ресурсов. С этой целью обе функции связаны с деятельностью в условиях неопределенности или риска на основе прогнозирования атак, защиты от них и знания того, что делать в случае атаки, и таким образом управление рисками становится общим знаменателем, соединяющим обе области. Физическую безопасность и кибербезопасность также объединяет понимание того, что даже самые действенные меры защиты не полностью предотвратят преодоление атакой средств защиты организации, какими бы сложными или надежными те ни были. Наконец, при обращении к сценариям, которые могли бы проиллюстрировать, где заканчивается кибербезопасность и начинается физическая безопасность или наоборот, быстро стало очевидно, что физическую и цифровую сферу, возможно, не настолько легко разделить, как это может показаться на первый взгляд.

66. **На практике физическая безопасность и кибербезопасность пересекаются.** В настоящее время системы, обеспечивающие функции безопасности и защиты, которые не используют в той или иной форме ИКТ, составляют скорее исключение, чем правило. В результате последствия нарушений кибербезопасности, затрагивающие такие системы, могут материализоваться в физическом мире, иногда в такой степени, что серьезной опасности подвергается жизнь или физическая целостность людей. Нет недостатка в примерах того, как кибербезопасность и физическая безопасность пересекаются на практике. Например, хакеры могут взять под свой контроль шлюз безопасности, использовать слабые места в протоколах безопасности, чтобы разместить шпионское ПО на электронных устройствах или загрузить конфиденциальную информацию на портативные устройства, получить онлайн-доступ к планам служебных помещений с целью выбора целей для вооруженного нападения, или похитить личные данные, чтобы заманить других в ситуации, когда они в конечном итоге невольно подвергают себя опасности, полагаясь на информацию из обычно надежных источников, мошенническим образом перехваченных киберпреступниками. Кроме того, ненадежные меры безопасности, ставящие под угрозу защиту помещений, центров обработки данных, серверных комнат или цифровых точек доступа от несанкционированного доступа или других форм неразрешенного вмешательства, исходящего от физических опасностей (природных или техногенных), могут иметь прямые неблагоприятные последствия, проявляющиеся в цифровой сфере. Сближение обоих миров может быть еще более выраженным в тех отделениях на местах, которые, как правило, дальше отстоят от центральных механизмов контроля и мониторинга кибербезопасности, а также являются потенциально более привлекательной целью, поскольку хранимая информация имеет прямое значение для жизни и здоровья людей. Примером этого могут быть данные о местонахождении или перемещении персонала в менее защищаемых местах.

67. **Институциональные связи между физической безопасностью и кибербезопасностью остаются спорадическими.** Ответы участвующих организаций на анкеты ОИГ и последующие беседы с должностными лицами выявили разную степень осознания взаимосвязи между физической сферой и кибер-сферой. Организационная архитектура только двух организаций отражает фактическую интеграцию структур обеспечения физической охраны и безопасности и кибербезопасности либо путем сосредоточения обеих функций в одном департаменте, подчиненном заместителю исполнительного главы с общим мандатом в области безопасности организации (ВОИС), либо путем стратегического определения обеих функций как двух среди многих элементов более широкой «системы управления организационной устойчивостью», которая объединяет средства защиты от всех видов угроз, будь то физические, цифровые, политические, природные или прочие (МСЭ). Другие организации признали наличие точек соприкосновения и полезных синергий и в определенной степени формализовали координацию и обмен информацией между обоими функциональными направлениями, например, с помощью двойного подчинения, совместных брифингов для старшего руководства или совместного участия в совещаниях либо обеспечения равного участия обоих направлений в корпоративных процессах, таких как управление рисками или планирование непрерывности деятельности, или на разовой основе в ситуациях кризисного реагирования, требующих участия обоих. Кроме того, уже осуществляется сотрудничество по конкретным мерам оперативного уровня (например, объединение информации о кибер- и физических угрозах в рекомендациях для командируемых в миссии или совместная разработка сложных технологических решений для удостоверений личности персонала и пропусков), с некоторыми осязаемыми преимуществами для обеспечения безопасности соответствующих организаций. Даже в тех организациях системы, где физическая защита и безопасность отделяются от киберпространства и считаются по сути не связанным с ним, организации сообщили об эпизодических неформальных контактах между обеими областями. Тем не менее для большинства организаций, опрошенных по этому поводу, реальность остается в том, что связь между физической безопасностью и кибербезопасностью недооценивается или признается лишь частично, что также имеет место на общесистемном уровне (пп. 159–164).

68. **Повышение уровня квалификации специалистов по кибербезопасности подразделений физической охраны и безопасности.** По мнению инспекторов, имеются возможности дальнейшего сближения между физической безопасностью и кибербезопасностью в интересах обеих областей и устойчивости организаций в более широком смысле. Один из вариантов — проработка возможности наращивания внутреннего потенциала за счет повышения уровня квалификации и расширения номенклатуры специальностей критического числа специалистов по безопасности и защите и включения владения вопросами кибербезопасности в будущие требования к таким сотрудникам, в частности, путем переработки нынешнего описания должностных обязанностей (например, дополнениях их элементами обработки информации о киберугрозах, моделирования угроз и аналогичных аналитических познаний). Представление о том, что кибербезопасность по сути не связана с обязанностями таких специалистов и отделена от них, может отчасти основываться на давней практике их набора в основном из числа сотрудников полиции и военнослужащих — представление, которое не учитывает, что последние уже получают современные познания в таких областях. Такие специалисты есть, и нет трудностей с их привлечением организациями системы Организации Объединенных Наций. После его создания этот дополнительный потенциал будет дополнять, а не заменять развитый и хорошо отлаженный механизм нынешней традиционной группы сотрудников безопасности и позволит им более эффективно взаимодействовать со специализированным потенциалом кибербезопасности в соответствующих организациях. Инспекторы признают, что эти две области обладают разными узкоспециализированными возможностями, которые хорошо развиты для достижения соответствующих целей защиты, и что, таким образом, попытки объединить их в одну структуру или включить одну в другую без дальнейшего изучения выглядят нецелесообразными. Однако усилия по расширению имеющихся возможностей для улучшения связей между обеими областями могут быть одним из элементов для изучения с целью достижения более целостного подхода к защите персонала и ресурсов организации, как это предусмотрено в рекомендации 5.

D. Формирование нормативной базы для соблюдения требований и подотчетности

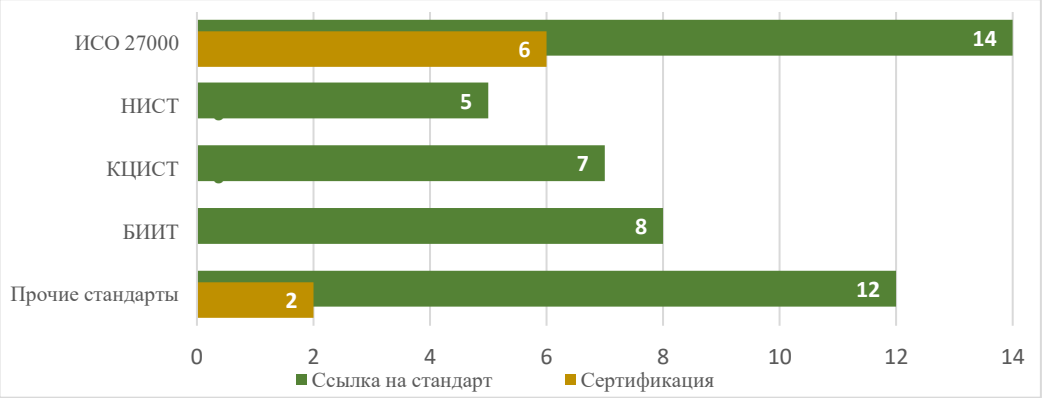
Отраслевые стандарты информационной безопасности

69. **Стандарты, используемые участвующими организациями.** Кибербезопасность — область, в которой был разработан ряд национальных и международных отраслевых стандартов, содержащих рекомендации и контрольные параметры с целью построения устойчивых систем управления информационной безопасностью. Этот термин, введенный Международной организацией по стандартизации, относится к совокупности мер — управленческих, нормативных и технологических, — которые отражают подход организации к кибербезопасности. Он охватывает сложный набор средств контроля, от правил и директив до средств и процессов управления, концепций безопасности, стратегий управления рисками и т. п. Участвующие организации называли самые разнообразные стандарты такого рода, иногда более одного, которые, как они указали, были отобраны исходя из их соответствия конкретным условиям и требованиям каждой организации и доработаны путем отражения тех контрольных параметров конкретного стандарта, которые были наиболее актуальны, в специально разработанном «положении о применимости». Инспекторы напоминают, что уже десять лет назад, в 2011 году, Сеть информационно-коммуникационных технологий одобрила соблюдение стандарта ИСО 27001 для учреждений системы Организации Объединенных Наций[16], а в 2017 году Специальная группа по информационной безопасности подтвердила эту позицию. Настоящий обзор подтверждает, что большинство организаций системы Организации Объединенных Наций либо уже сертифицированы или планируют пройти сертификацию в соответствии с ИСО 27001, либо самостоятельно решили привести свою систему в соответствие с ним, не обращаясь за официальной сертификацией. Наряду

[16] CEB/2011/HLCM/ICT/16.

с ИСО 27001 имеется несколько других стандартов, используемых организациями системы Организации Объединенных Наций, которые отражены на диаграмме VI ниже и дополнительно описаны в приложении III. Только три организации не назвали каких-либо стандартов и не предоставили информацию по этому поводу.

Диаграмма VI
Основные отраслевые стандарты, используемые организациями — участницами ОИГ



Источник: Анкета ОИГ (2020) и беседы.
Сокращения: НИСТ — Национальный институт стандартов и технологий Соединенных Штатов; КЦИСТ — Контрольные цели для информационных и связанных технологий; БИИТ — Библиотека инфраструктуры информационных технологий.

70. **Официальная сертификация по сравнению со ссылками на стандарты.** Что касается полезности официальной сертификации по сравнению с менее строгими формами добровольного соблюдения стандартов, то инспекторы убедились в том, что у экспертов по этому поводу есть разные мнения. С одной стороны, руководство может принять решение о сертификации организации для предоставления надежных гарантий директивным и руководящим органам, а также внешним партнерам, исходя из официального характера процесса и акта сертификации, а также его строгости, предусматривающей ежегодный независимый аудит для продления сертификации. Она также может служить повторяющимся импульсом инноваций в свете необходимости демонстрировать постоянные улучшения. В то же время некоторые организации утверждают, что сертификация может быть слишком затратной и сложной, чтобы оправдать вложения. Они также критикуют ее сильную зависимость от формального соответствия, что может стимулировать составление приукрашенной, а не реалистичной отчетности. Инспекторы признают, что сертификация и согласование со стандартом могут быть полезными вариантами, особенно на разных этапах постепенного наращивания киберзащиты, тем более что стандарты могут использоваться по-разному, в том числе в качестве эталона или основы для целей аудита, внутренней дорожной карты для самосовершенствования, дополнительного стимула для соблюдения мер контроля или образца или реперной системы, служащей основой для индивидуализированных подходов.

71. **Преимущества ссылки на стандарты.** Инспекторы воздерживаются от аргументов в пользу конкретного отраслевого стандарта или согласованного общесистемного подхода, поскольку разные стандарты могут надлежащим образом служить разным целям и предоставлять подходящие варианты для разной степени развития. Таким образом, нет одного правильного стандарта, как и одного правильного способа обеспечения кибербезопасности, но есть веские основания черпать вдохновение — формально или неформально — в соответствующих отраслевых стандартах при создании и использовании собственной нормативной базы. Таким образом, участвующие организации должны определить соответствующий стандарт, а в его рамках — наиболее подходящие средства контроля, исходя из уровня защиты, соответствующего их ситуации, с учетом требований и рисков, выявленных после надлежащей оценки рисков для кибербезопасности данной организации. Воздерживаясь от комментариев, инспекторы отмечают, что решение организации по

этому поводу может также иметь последствия для всей системы, где использование одной и той же основы или стандарта может облегчить сопоставимость и дать общий язык для всех. Наоборот, различные подходы в контексте межучрежденческих механизмов могут предоставить дополнительные возможности межорганизационных дискуссий, проверки допущений, более критического анализа собственного выбора в сравнении с выбором других и взаимного обучения в более общем плане, что в конечном итоге приносит пользу организациям по отдельности.

Основы политики и процедуры

72. **Создание соответствующей нормативно-правовой базы составляет прерогативу каждой организации.** Кроме разнообразных отраслевых стандартов, упомянутых выше, не имеется какой-либо общеприменимой авторитетной системы регулирования в вопросах кибербезопасности. Отсутствие международно-правового акта или единого подхода в этой сфере можно объяснить тем, что сама она многогранна и сложна для разграничения и как таковая представляет сложность для регулирования даже для законодательства какого-либо одного государства. Эта сложность еще более возрастает, если подняться на международный уровень, где еще труднее определить общие нормы, регулирующие отношения между государствами, а также другими заинтересованными сторонами государственного и частного сектора, действующими в киберпространстве. На данный момент нет ни юридически обязательного акта в международном праве, ни единой нормативной базы для организаций системы Организации Объединенных Наций, конкретно регулирующей кибербезопасность. Как следствие, международную структуру управления киберпространством лучше всего можно охарактеризовать как лоскутное одеяло формальных и неформальных институтов и норм, состоящих из пересекающихся и частично совпадающих технических стандартов, контрактов, законов и межправительственных решений. В отсутствие согласованной структуры, которая могла бы служить моделью, каждая организация сохраняет за собой прерогативу — в пределах параметров, продиктованных ее уставом и соответствующими решениями директивных и руководящих органов — формулировать свои собственные правила при относительной самостоятельности и выбрать свой план кибербезопасности.

73. **Обычное упоминание кибербезопасности в стратегиях ИКТ.** Охват кибербезопасности ныне действующей нормативно-правовой базой, иными словами, нормативная база, в которой действуют функциональные подразделения организаций, может быть разным и часто отражает историческую эволюцию кибербезопасности как области, которая зародилась в сфере ИКТ и выделилась в отдельную дисциплину. Некоторые организации воспринимают кибербезопасность совершенно независимо от ИКТ, рассматривая ее как самостоятельный вопрос наравне с физической безопасностью (ВОИС) или как элемент более широкого видения повышения устойчивости организации (МСЭ), но такие подходы остаются исключением. Большинство участвующих организаций разработали многолетний общеорганизационный стратегический документ, в котором излагается их видение ИКТ, и в подавляющем большинстве в этих стратегиях ИКТ отражены соображения кибербезопасности. При этом некоторые из них содержат только базовую справочную информацию, иногда дополняемую более сложными руководящими указаниями более низкого уровня, в то время как другие содержат целые главы, посвященные данной теме. **Независимо от степени проработки руководящих указаний по кибербезопасности в рамках более широких стратегий организаций в области ИКТ, инспекторы сочли наличие упоминаний этого вопроса в таких стратегиях ИКТ положительным первым шагом.**

74. **Действие или разработка директив, специально посвященных кибербезопасности, во многих участвующих организациях.** Следует отметить, что основные документы нескольких ведущих отраслевых стандартов требуют принятия определенных директив и документально зафиксированных процедур в области кибербезопасности в качестве ключевого элемента контроля, составляющего основу

системы обеспечения информационной безопасности организации[17]. Настоящий обзор показал, что многие организации подготовили такие специальные руководящие указания, а организации, которые этого еще не сделали, за некоторыми исключениями, находятся в процессе их разработки. В частности, по имеющимся сведениям, 17 организаций приняли регулирующие документы, прямо касающиеся кибербезопасности (3 из которых в настоящее время пересматриваются), а 4 подтвердили, что находятся в процессе разработки новых директив. Только три организации сообщили, что они не разработали и не начали разработки конкретных директив или правил кибербезопасности, и используют для решения этих вопросов свои правила и процедуры в области ИКТ. Таким образом, можно сказать, что, за некоторыми исключениями, организации осознали важность наличия четко сформулированной системы координат, направляющей их подход к кибербезопасности. В приложении IV перечислены ключевые инструменты, регулирующие кибербезопасность в рамках нормативной базы участвующих организаций.

75. **Сложность, разнородность и многоуровневость системы как общее правило.** Независимо от создания в рассматриваемых организациях более проработанных систем регулирования в области кибербезопасности или использования в них систем, обычно применяющихся в области ИКТ, как могли убедиться инспекторы, такие правила, как правило, разбросаны в разнообразных стратегических, директивных, процедурных и технических руководящих документах. Терминология таких документов различается в разных участвующих организациях: от стратегий до документов о постановке задач, директив, административных инструкций, пошаговых описаний процедур, руководящих положений, правил работы и протоколов, которые часто концептуально пересекаются или даже используются взаимозаменяемо. Международный вычислительный центр Организации Объединенных Наций разработал модель представления различных нормативных элементов Системы обеспечения информационной безопасностью в виде уровней с максимальной степенью абстрагирования на верхнем уровне и максимальной степенью детализации на нижнем уровне, и оказал поддержку нескольким организациям системы Организации Объединенных Наций в оценке и совершенствовании созданных теми систем регулирования и управления. Основываясь на этой модели, в приложении IV представлен обзор целей, форматов и типичного содержания документов о кибербезопасности и ИКТ, рассмотренных инспекторами, при признании того, что подробный качественный анализ содержания по всем участвующим организациям вышел бы за рамки настоящего обзора.

76. **Адаптация к условиям и периодический обзор.** Обеспечение того, чтобы правила отражали специфику организации, может включать их корректировку в необходимых случаях для точного отражения мер контроля, требуемых отраслевыми стандартами, которым организация решила следовать. Пример этого был найден в ВПП и Программе развития Организации Объединенных Наций (ПРООН), где каждой мере технического контроля стандарта ИСО 27001, с которым организация увязала свое «положение о применимости», соответствует правило ее системы норм регулирования. Это также может включать области регулирования, вызывающие особую озабоченность, которые могут иметь разную степень актуальности для организаций, например, руководство по безопасным методам разработки своими силами веб-сайтов, баз данных или приложений. Таким образом, наблюдаемое разнообразие правил и различия в нормативно-правовой базе может быть убедительно объяснено, по крайней мере частично, их адаптацией к конкретным условиям организации, а не восприниматься как признак отсутствия систематического подхода

[17] В стандарте ИСО 27001 нормативный перечень целей управления начинается с элемента управления A.5 «Правила информационной безопасности», где указывается, что необходимо разработать систему правил и довести их до сведения сотрудников и соответствующих внешних сторон. Национальный институт стандартов и технологий Соединенных Штатов в своем основном документе «Система повышения кибербезопасности критически важной инфраструктуры» в рамках категории управления указывает, что «правила, процедуры и процессы» задают направление «менеджмента рисков кибербезопасности».

к регулированию. Кроме того, в динамичной области кибербезопасности еще более важно, чтобы нормативные руководящие положения оставались адаптируемыми и актуальными, чего некоторые организации пытались достичь с помощью их периодического пересмотра. В этом отношении хорошей практикой можно считать включение в такие руководящие документы и директивы точных сроков, в течение которых они должны быть официально рассмотрены и пересмотрены по мере необходимости, с указанием того, кто несет ответственность за начало такого процесса.

77. **Важность руководящих положений независимо от масштабов, степени разработки или организационной структуры.** В свете значительного разнообразия вопросов, связанных с кибербезопасностью, которые могут требовать регулирования, трудно описать, не говоря уже о том, чтобы рекомендовать их, конкретные правила или процедуры, могли бы оптимальным образом обеспечивать надежную систему кибербезопасности. Достаточно сказать, что наличие даже базовых руководящих положений в этой часто высокотехнологичной и многогранной области важно для обеспечения согласованности и последовательности в применении мер безопасности, независимо от масштабов организации или ресурсов, которыми та располагает.

Кибербезопасность как проблема всей организации

78. **Кибербезопасность как общеорганизационная проблема.** При разработке нормативной базы, необходимой для повышения киберустойчивости организаций было бы недальновидно останавливаться только на правилах, конкретно посвященных ИКТ и кибербезопасности. Поддержание киберзащиты организации составляет общую обязанность многих подразделений, и отношение к ней как к общеорганизационной задаче может иметь большое значение для достижения внутренне вызревшего, а не навязанного общеорганизационного подхода (пп. 92–95). Имеются признаки того, что ряд организаций уже начали учитывать соображения кибербезопасности в своих разнообразных директивных документах. Однако оценка степени отражения проблематики кибербезопасности в общей нормативно-правовой базе участвующих организаций потребует гораздо более широкого анализа и более глубокого изучения, чем позволяет настоящий обзор. Инспекторы предлагают несколько указателей, рассмотренных во вставке 4.

Вставка 4
Указатели для отражения кибербезопасности в нормативно-правовой базе организации

- Элементы, относящиеся к кибербезопасности, могут быть включены непосредственно в правила, практику и процессы, направляющие работу таких подразделений, как подразделения кадров, закупок, связи или юридического обеспечения. Два примера последнего — включение в сборник инструкций по закупкам конкретных требований проверки при привлечении внешних поставщиков услуг и включение в шаблоны проектных документов или в руководящие документы по программам, используемые подразделениями в своей повседневной работе, шагов, которым необходимо следовать при управлении киберрисками на протяжении всего жизненного цикла проекта.
- Роли и обязанности подразделений или служб, помимо тех, которые непосредственно связаны с ИКТ или кибербезопасностью, могут быть поручены и прямо отражены в основных действующих регулирующих документах. Так, в директиве ВПП о безопасности информационных технологий детализируются функции и обязанности различных категорий лиц, таких как владельцы информации, хранители информации, пользователи информации, руководители и персонал. Еще один пример — ВОИС.

- Могут быть определены пути, с помощью которых все соответствующие заинтересованные стороны, помимо сотрудников ИКТ и кибербезопасности, должны будут регулярно вносить вклад не только в разработку этих документов, но и в их осуществление (например, путем включения представителей таких заинтересованных сторон в качестве членов в соответствующие органы внутреннего управления или разработки процесса утверждения правил, требующих проведения консультаций с определенными заинтересованными сторонами до утверждения окончательного текста).

Источник: Подготовлено ОИГ.

Соблюдение правил и подотчетность

79. **Доступность как условие соблюдения правил.** Самая четко сформулированная нормативно-правовая база эффективна лишь в той степени, в которой ее соблюдают соответствующие стороны. На соблюдение таких правил могут влиять несколько факторов, в том числе наличие материалов, в которых четко изложено, что требуется от каждой заинтересованной стороны и каждого сотрудника и почему. Этот последний момент был подчеркнут одним из руководителей службы информационной безопасности, с которым беседовали инспекторы, который особо отметил, что проблема заключается не столько в отсутствии письменных инструкций, сколько в плохом понимании пользователями того, почему эти инструкции существуют, что они защищают и как их незнание и несоблюдение может повлиять как на пользователя, так и на организацию. Важность этой осведомленности дополнительно раскрывается в других частях настоящего доклада (пп. 97–103) и включает необходимость простого, нетехнического и доступного изложения мыслей, главная задача которого — рельефно обозначить последствия рискованного киберповедения для пользователя. Пример хорошо организованного хранилища полного набора установочных материалов по кибербезопасности, включая видеоролики с понятным изложением, плакаты, краткие практические статьи, вопросы и ответы и полный набор действующих правил и установок, сгруппированных по темам и дополненных пояснительными примечаниями, был найден в Секретариате Организации Объединенных Наций, где на него можно пройти одним щелчком мыши с главной страницы в интранете Управления информационно-коммуникационных технологий.

80. **Возможная неадекватность нынешнего ответа на несоблюдение требований кибербезопасности.** Важный фактор — который вполне может повлиять на соблюдение правил — наличие действенных санкций, которые могут быть применены в случае несоблюдения, в идеале подкрепленных знанием и ожиданием того, что несоблюдение правил повлечет за собой. Несколько правил, рассмотренных инспекторами, содержали конкретные формулировки о санкциях за нарушения кибербезопасности. Даже в тех случаях, когда в соответствующих правилах упоминаются конкретные санкции, собранная информация об их применении на практике указывает на то, что они редко применяются, и, как следствие, сотрудники, совершающие рискованные действия, обычно не привлекаются к ответственности. В большинстве участвующих организаций некоторые конкретные положения о санкциях за нарушения правил использования ИКТ, которые обычно включают нарушения кибербезопасности, могут содержаться в правилах разрешенного использования ресурсов ИКТ. Как правило, такие нарушения влекут за собой те же дисциплинарные меры, которые предусмотрены в отношении нарушения любых других правил или положений о персонале. Однако обычные процессы, даже если они действительно применены и завершены, как известно, медленны, громоздки и затратны и, как правило, задействуются только в случаях особо вопиющих нарушений, связанный с ИКТ.

81. **Необходимо рассмотреть систему более нюансированных санкций.** В случае нарушений кибербезопасности, которые часто происходят из-за простого незнания или небрежности, **инспекторы считают, что более многообещающим подходом могут быть более легкореализуемые и менее формальные и жесткие санкции**.

Такие санкции позволили бы сразу решать проблему более непосредственным образом, соизмеримым с серьезностью нарушения. Тем не менее необходимо найти баланс, обеспечивающий чтобы последствия нарушения по-прежнему в достаточной степени ощущались тем, кто их допустил, чтобы поощрять более строгую кибергигиену и более ответственное поведение. Неявное признание этого можно обнаружить в практике некоторых организаций, которые проводят различие между незначительными и более серьезными нарушениями их соответствующих правил кибербезопасности. Однако было не столь очевидно, удалось ли им отразить это различие в санкциях, которые бы в первую очередь касались незначительных нарушений, но оставались бы действенными. Например, некоторые правила предусматривают информирование прямых руководителей или руководителя подразделения ИКТ, что может представлять собой единственную имеющуюся возможность «мягкого» воздействия с целью соблюдения требований, но не предполагает каких-либо последствий, кроме возможной неловкости. Контрпример, который стоит отметить в силу его специфики и прямого отрицательного воздействия на пользователя без чрезмерного наказания, приводится МАГАТЭ, которое предусматривает в своих правилах прямые недисциплинарные санкции в виде отзыва права доступа пользователей, не соблюдающих правила, к информационным системам. Кроме того, следует отметить, что эти правила признают необходимость соразмерности, требуя знания о них как условия наказания за нарушение, и уравновешивают цель действенной защиты ресурсов организации с целью обеспечения того, чтобы санкции не влекли за собой мелочного контроля над персоналом. На практике отзыв осуществляется на временной основе и после неоднократных предупреждений. Инспекторы хотели бы подчеркнуть, что любой действенный механизм санкций не может быть реализован без прямой поддержки со стороны исполнительного главы, что является одним из факторов успеха приведенного примера. **По мнению инспекторов, исполнительным главам следует также изучить возможность введения мер поощрения за сообщение об инцидентах и принятие людьми ответственности за свои небезопасные или рискованные действия.** При этом будет важно найти способы согласования цели сдерживания с помощью более нюансированных санкций с целью поощрения людей сообщать об инцидентах, не опасаясь последствий.

E. Использование вклада надзорных механизмов

82. **Аудит и надзор на всех уровнях с вниманием к кибербезопасности.** Инспекторы изучили практику решения надзорными органами вопросов кибербезопасности в контексте их соответствующих сфер деятельности, будь то на уровне службы внутренней ревизии (направленной в первую очередь на оценку соблюдения правил и процедур), на уровне внешней ревизии (в основном связанной с финансовым аудитом и проверкой соблюдения правил, а иногда и с проверками эффективности в административной и управленческой областях) или на уровне комитетов по аудиту и надзору (в основном консультирующих по более общим вопросам, заслуживающим первоочередных действий и внимания со стороны высшего руководства, а также директивных и руководящих органов). Инспекторы приветствуют то, что на каждом из этих уровней кибербезопасность является предметом интереса в течение последних пяти лет, а в некоторых организациях — даже дольше.

Рассмотрение вопросов кибербезопасности надзорными органами

83. **Внутренний и внешний аудит в основном заострен на ИКТ, включая в определенной степени кибербезопасность.** Вопросы, связанные с ИКТ, как правило, хорошо вписываются в планирование внутреннего аудита с учетом рисков. Однако в ходе своего исследования ОИГ обнаружила лишь ограниченное количество аудиторских заданий, конкретно посвященных кибербезопасности, в последние пять лет. Что касается штата сотрудников для выполнения таких заданий, то только несколько организаций имеют в своем штате сотрудников в области аудита ИКТ, в то время как большинство организаций в основном привлекают внешних экспертов.

В большинстве случаев такой подход представляется удовлетворительным. На протяжении многих лет во многих участвующих организациях ИКТ также были областью внимания для внешних аудиторов, которые занимались такими темами, как непрерывность деятельности, оценка рисков и управление рисками, правила в области ИКТ и управление ресурсами ИКТ. В целом ответы руководителей, с которыми проконсультировались инспекторы, свидетельствовали о принятии полученных рекомендаций и указывали на меры, принятые для их выполнения.

84. **Уделение пристального внимания кибербезопасности комитетами по аудиту и надзору.** В 2016 году представители комитетов по надзору 19 организаций системы Организации Объединенных Наций «определили, среди прочего, риски для кибербезопасности в цифровой среде как приоритетной области и согласились с необходимостью рассмотреть понимание их руководством и его готовность действовать сообразно с ними»[18]. В этой связи анализ содержания докладов этих комитетов показывает, что постоянное внимание уделялось усилению аспектов управления и управления рисками кибербезопасности, хотя ни один из них не содержит конкретного упоминания кибербезопасности в своем круге ведения, и только четыре упоминают в нем ИКТ. Комитеты в основном рассматривали такие вопросы в рамках своего мандата по общеорганизационному управлению рисками или, где это применимо, при отслеживании состояния выполнения рекомендаций внутреннего или внешнего аудита, связанных с ИКТ. Настоящий обзор показал, что специалисты в этой области не всегда присутствовали в составе комитетов по аудиту и надзору, поскольку только четыре комитета, по-видимому, имели в своем составе таких специалистов, в то время как большинство из них привлекали на разовой основе внешних консультантов, по схеме, аналогичной принятой для внутренней ревизии. Похвально, что эти комитеты изучают эту тему не только потому, что это может помочь руководству в реализации подхода к кибербезопасности, основанного на оценке рисков, но и потому, что это способ информирования директивных и руководящих органов о соответствующих рисках кибербезопасности, что позволяет тем вносить свой вклад в уменьшение рисков организации.

Значение рекомендаций надзорных органов для улучшения состояния кибербезопасности в организациях

85. **Рекомендации надзорных органов, способствующие позитивным структурным сдвигам.** Участвующие организации сообщили, что существенные структурные сдвиги в их подходе к кибербезопасности были вызваны замечаниями надзорных органов, что подчеркивает отдачу таких механизмов. Во время бесед должностные лица, отвечающие за ИКТ и кибербезопасность, обычно оценивали доклады о надзоре как импульс для изменений благодаря повышению понимания высшим руководством необходимости уделять больше внимания надежности кибербезопасности. Инспекторы действительно обнаружили примеры, когда рекомендации внутренней ревизии непосредственным образом способствовали усилению кибербезопасности в соответствующей организации, например в ВОИС. Другие примеры были найдены в ИКАО и ЮНФПА, где рекомендация ревизоров привела к разработке многолетней дорожной карты; в ЮНЕСКО, где была введена должность главного сотрудника по информационной безопасности; или в Секретариате Организации Объединенных Наций, где значительно повысилось соблюдение требований прохождения учеб по информационной безопасности. За последние пять лет внешние аудиторы также изложили рекомендации по вопросам, связанным с кибербезопасностью, для 16 участвующих организаций, в частности, в отношении соблюдения требований обучения по вопросам информационной безопасности, восстановления данных, контроля доступа пользователей и ресурсов, предназначенных для обеспечения кибербезопасности. Полезность рекомендаций аудита, по-видимому, лучше осознается, когда они выходят за рамки подхода к соблюдению требований к эксплуатационным и техническим аспектам и вместо этого предлагают стратегические улучшения, признавая, что простое соблюдение нормативно-правовой базы не означает защиты. В то же время многие организации

[18] См. A/72/295, пп. 40–43.

выразили озабоченность по поводу того, что в таких рекомендациях иногда недостаточно учитывались ресурсные ограничения и реальные условия деятельности, что уменьшало вероятность выполнения некоторых из них.

86. **Необходимость специалистов по кибербезопасности для систематического обеспечения надзорных функций.** Чтобы гарантировать максимальную отдачу надзорных органов в области кибербезопасности, важно, чтобы они имели и хорошо понимали всю соответствующую информацию, касающуюся связанных с этим рисков, возможностей и ограничений внутри организации. Самый эффективный способ этого — обеспечить, чтобы знания и опыт специалистов по кибербезопасности в организации могли быть задействованы в работе надзорных подразделений. Имеется множество вариантов этого, некоторые из которых уже укоренились в практике или даже в нормативно-правовой базе участвующих организаций, по отдельности или в сочетании, и могут считаться передовой практикой. К ним относятся следующие: a) обязательное проведение консультаций с главным сотрудником по информационной безопасности или соответствующим подразделением при планировании аудита с учетом рисков и их активное привлечение к определению соответствующих средств контроля и показателей; b) предоставление надзорным органам информации о кибербезопасности согласно требованиям их соответствующих мандатов как в докладах о статистике инцидентов, так и на специальных или регулярных брифингах или с помощью других средств; и c) передача любого доклада или любой рекомендации ревизоров по вопросам кибербезопасности для комментариев главному сотруднику или подразделению по информационной безопасности до их окончательной доработки для уменьшения озабоченности по поводу того, что рекомендации недостаточно отражают реальности организации и поэтому неосуществимы.

F. Привитие культуры кибербезопасности сверху вниз

87. **Руководство должно поощрять признание ошибок и уязвимостей.** Как обсуждалось выше, надежное состояние кибербезопасности в организации также является вопросом мощной внутренней культуры, которая начинается с внимания и приоритета, уделяемого проблеме со стороны исполнительного руководства, — тона наверху. Тем не менее на этом все не заканчивается и должно быть доведено до каждого сотрудника. Для этого необходимы постоянная заинтересованность и участие высших эшелонов организации, которые должны выходить за рамки простых заявлений об отнесении кибербезопасности к числу приоритетов организации. Главным элементом будет поощрение внутренней культуры, в которой признание возникновения инцидентов рассматривается не как неудача, а как отправная точка для решения общей проблемы и усиления защиты организации и ее ресурсов, для чего необходимо продемонстрировать совместную и индивидуальную ответственность за ошибки и слабости. В этой связи что-то можно почерпнуть из культуры правоохранительной деятельности в области физической защиты и безопасности, где возникновение инцидентов считается само собой разумеющимся, и ожидается, что о них будут сообщать и разбираться в обычном порядке, без предвзятости. **Инспекторы считают обязанностью исполнительного главы привитие такой культуры во всех подразделениях и во всех местах присутствия организации, поскольку информационные системы взаимосвязаны и взаимозависимы, а атака или несанкционированный доступ в любом месте могут привести к нарушению безопасности повсюду.**

88. **Осведомленность и подотчетность высшего руководства как отправная точка.** Первый шаг на пути к формированию нового мышления и культуры — осознание самим высшим руководством рисков, связанных с кибербезопасностью, и выработка понимания последствий бездействия и плохой кибергигиены на основе возросшего интереса к этому вопросу. Этого можно достичь, запрашивая регулярные брифинги у соответствующих должностных лиц внутри организаций, таких как эксперты по кибербезопасности, сотрудники по управлению рисками и представители надзорных органов, а также с помощью инициатив по обучению и повышению

осведомленности, специально предназначенных для старшего руководства. С 2020 года в Секретариате Организации Объединенных Наций договоры, заключаемые между Генеральным секретарем и старшими должностными лицами, содержат положения, направленные на повышение осведомленности и подотчетности в этой области. Последовательность и эффективность договоров и показателей деятельности, содержащихся в них, выходят за рамки настоящего обзора, но привязка целей кибербезопасности к служебной аттестации руководителей высшего звена стала нужным шагом на пути к повышению подотчетности и установлению правильного тона на высшем уровне. Кроме того, следует поощрять, в том числе в каждой участвующей организации, такие инициативы, как сообщение в Комитете высокого уровня по вопросам управления, предупредившее высшее руководство о продолжающемся воздействии рисков для кибербезопасности на деятельность организаций, не только в плане нарушения административных систем, сетей и инфраструктуры, но и в плане подрыва осуществления основной деятельности, предусмотренной в мандате[19].

89. **Одни деньги не купят культуры кибербезопасности.** Есть много способов, которыми исполнительное руководство может вдохновить на действия и конкретным образом повлиять на образ мышления по всей цепочке управления. Во-первых, значение, придаваемое кибербезопасности, может быть выражено в виде адекватного распределения ресурсов. В то же время одни деньги не могут решить проблемы обеспечения кибербезопасности, и они не могут купить культуры кибербезопасности. В частности, финансовая поддержка не освобождает исполнительное руководство от его ответственности за обеспечение активного руководства в вопросах кибербезопасности, что подтверждает недавний доклад известного аналитического центра по кибербезопасности «Гартнер»[20]. Выражение поддержки только в финансовых терминах может на деле перенести ответственность исполнительного руководства на следующий более низкий уровень, где средства могут вкладываться без общего стратегического видения. Распределение ресурсов и связанные с ними вложения должны осуществляться в контексте процессов организации, а не с чисто технологической точки зрения или с точки зрения управления рисками, и исполнительное руководство лучше всего может принять обоснованное решение, должным образом взвесив все соображения (пп. 108–109).

90. **Неденежные способы демонстрации поддержки на уровне руководства.** Некоторые примеры передовой практики участвующих организаций в области реальной неденежной поддержки со стороны высшего руководства включают следующие действия, предпринятые исполнительными главами: активное участие в программах повышения осведомленности, например, путем записи видео-заявлений о поддержке; выступления по вопросам кибербезопасности перед сотрудниками на общих собраниях; обсуждение с сотрудниками кибератак на личном опыте; публичное ролевое моделирование рекомендованного поведения; поддержка частых и регулярных имитационных фишинговых кампаний для сотрудников всех уровней, включая руководителей высшего звена; обеспечение передачи ответственности на нижний уровень путем привлечения старших руководителей к участию в обучении и предъявления своим подчиненным требований по соблюдению правил и утвержденного порядка действий; поддержка применения соразмерных санкций, особенно для «рецидивистов», которые продолжают нарушать правила и процедуры кибербезопасности. Как указано выше, отправной точкой служит признание возможности ошибок и извлечение уроков из них, а также совместное устранение их последствий.

91. **Необходимость времени, последовательного курса и поддержки на высоком уровне для изменения менталитета.** Чтобы они укоренились в установках сотрудников на всех уровнях и тем самым сформировали организационную культуру кибербезопасности, такие меры придется повторять, и для того, чтобы они дали результаты, потребуется время. Опыт показывает, что шансы на успех как возрастают,

[19] См. CEB/2017/HLCM/ICT/9.

[20] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.

так и приближаются, когда руководство организации последовательно указывает на важность кибербезопасности, которая не сводится к разовой капании. Как отмечалось на восьмом симпозиуме Специальной группы по информационной безопасности в 2019 году, «изменить поведение людей сложно, для этого требуется постоянный поток новой информации и периодическое переобучение, а также понимание латентных рисков технологий и последствий нарушения правил информационной безопасности»[21].

G. Внедрение общеорганизационного подхода

92. **Роль административных подразделений.** В русле растущего понимания того, что ответственность за кибербезопасность не может лежать только на подразделениях ИКТ, большинство участвующих организаций так или иначе признали, что административные, а также оперативные подразделения должны играть здесь свою роль. В большинстве организаций это понимание было более явно выражено в ответах на анкеты ОИГ в отношении административных подразделений. Фактически, независимо от того, отражено ли это формально в нормативно-правовой базе организации, ряд административных подразделений регулярно вносят свой вклад в поддержание общей защиты кибербезопасности организации. Это включает: подразделения кадров, содействующие организации программ обучения кибербезопасности; подразделения закупок, регулирующие взаимоотношения поставщиков с внешними поставщиками услуг, включая их проверку с точки зрения кибербезопасности; юридические подразделения, предоставляющие консультации по регулятивным, договорным или нормативным вопросам; подразделения общественных связей, занимающиеся отношениями с внешними заинтересованными сторонами. Естественно ожидать, что помимо их вклада, связанного с конкретными функциями, большинство этих подразделений будут предрасположены к учету соображений кибербезопасности в своей повседневной деятельности, поскольку их профильная деятельность связана с работой с конфиденциальной информацией, включая личные и финансовые данные. Происходит ли это в достаточной степени на практике и может ли это рассматриваться как отражение фактического понимания такими подразделениями своей особой роли по защите конфиденциальной информации, не очевидно из материалов, изученных ОИГ. Эта область может заслуживать повышенного внимания со стороны руководителей таких подразделений и внутренних аудиторов, и при необходимости может быть включена в оценки кибербезопасности, проводимые внешними поставщиками.

93. **Роль оперативных подразделений.** Информация, собранная в ходе подготовки настоящего обзора, предполагает, что, за исключением тех участвующих организаций, чьи мандаты устанавливают строгие требования конфиденциальности данных в качестве основного аспекта их работы, в оперативных подразделениях, в отличие от административных подразделений, руководители часто воспринимают кибербезопасность как административное бремя и препятствие для деятельности. Сообщается, что программные подразделения недостаточно восприимчивы к необходимости учета требований кибербезопасности и устойчивости при разработке и реализации своих проектов и мероприятий. По словам главного сотрудника по информационной безопасности, с которым была проведена беседа, «правила и процедуры кибербезопасности часто рассматриваются как препятствие для своевременного проведения работы, а не как щит, ограждающий репутацию и ресурсы организаций, а также эффективность их деятельности». На этом фоне особенно важно, чтобы исполнительные главы активно изживали те представления, что усиление мер кибербезопасности препятствует гибкости деятельности или достижению поставленных целей.

94. **Системный и ответственный подход к функциям и обязанностями как ключ к общеорганизационному подходу.** Как указывалось выше (п. 78), учет соображений кибербезопасности в правилах работы соответствующих подразделений

[21] CEB/2019/HLCM/DTN/02.

и их практике сам по себе будет признанием того, что каждое подразделение организации может внести свой вклад в достижение общеорганизационного подхода. В свете наблюдаемой в последнее время во многих организациях тенденции децентрализации и делегирования полномочий нижестоящим руководителям, учет таких соображений также внесет вклад в обеспечение более непосредственной ответственности и подотчетности в масштабах всей организации благодаря определению соответствующих обязанностей там, где каждой заинтересованной стороне будет проще ознакомиться с ними. Более четкое определение аспектов кибербезопасности программных и административных функций на основе их учета может уменьшить недопонимание и недостаток ответственности. Так, инспекторы отметили некоторую напряженность между экспертами по кибербезопасности и представителями других организационных подразделений, возникшую в результате восприятия ими своей роли в обеспечении надежного состояния кибербезопасности. **В этой связи инспекторы подчеркивают, что, в частности, оперативные подразделения должны брать на себя большую ответственность за аспект кибербезопасности в своей работе.** Однако участие подразделений не должно означать передачу ответственности исключительно им как кураторам рисков. Эксперты по кибербезопасности также не могут нести единоличной ответственности за защиту ресурсов организации, если на подразделения организации не ложится значительная часть бремени. Будет важно найти правильный баланс, и учет соображений кибербезопасности во всех областях работы организации может заложить основу для установления правильных взаимных ожиданий между различными подразделениями и их соответствующими ролями.

95. **Необходимость дальнейшего расширения ролевого обучения.** Полезный опыт, найденный в нескольких участвующих организациях, — возможности ролевого обучения кибербезопасности и меры по повышению осведомленности, которые следует и дальше расширять, чтобы все заинтересованные стороны имели оптимальные возможности вносить свой соответствующий вклад в киберустойчивость организации, который от них ожидается. На общесистемном уровне Сеть информационно-коммуникационных технологий уже поощряет привлечение к этому определенных групп пользователей в зависимости от их функциональных обязанностей, например сотрудников по общеорганизационному планированию ресурсов, специалистов по финансам и бухгалтерскому учету, сотрудников по закупкам и административных руководителей. Некоторые организации также разработали специальные занятия для сотрудников, выполняющих важные задачи, или для сотрудников, работающих на местах, которые сталкиваются с определенными рисками, связанными с определенными местами или инфраструктурой. Среди этих особых аудиторий, административные и старшие руководители, с одной стороны, и руководители программ, с другой стороны, возможно, заслуживают приоритетного внимания, поскольку их собственное понимание кибербезопасности и отношение к ней, вероятно, будет транслироваться внутри их соответствующей организации или организационной единицы и будет существенным образом способствовать — или препятствовать — формированию культуры кибербезопасности.

H. Сотрудники как создаваемая первая линия защиты

96. **«Человеческий фактор» — угроза, защита и основа культуры кибербезопасности и устойчивости.** Большинство организаций системы Организации Объединенных Наций приняли важные технические и практические меры по предотвращению и снижению риска кибератак (п. 38). Тем не менее среди экспертного сообщества кибербезопасности имеется консенсус в отношении того, что по-прежнему стоит задача разъяснения всем сотрудникам их роли в защите информации и цифровых ресурсов организации, а также важности придерживаться правил, процедур и передового опыта кибербезопасности. Во многих отношениях «человеческий фактор» приобрел значение в глобальном ландшафте угроз кибербезопасности, что отражается в растущей обеспокоенности участвующих организаций по поводу того, что отдельные конечные пользователи становятся все более уязвимыми для методов социальной инженерии (пп. 26–27). Также оказалось,

что воздействовать на него как источник риска особенно сложно. Помимо того, что он является одновременно первой линией защиты и самым слабым звеном в сети цифровой безопасности своей организации, каждый отдельный сотрудник также представляет собой важную опору организационной культуры кибербезопасности и устойчивости. Неблагоприятные последствия плохой киберпрактики многочисленны и часто проявляются в виде серьезных внутренних угроз. Они могут быть вызваны: ошибками, допущенными невнимательными или незаинтересованными пользователями; недостаточной осведомленностью или бдительностью (что часто используется в фишинговых атаках); неэффективностью методов защиты данных, таких как выбор ненадежных паролей или совместное использование параметров доступа несколькими пользователями; использованием несанкционированного или устаревшего ПО; разработкой приложений за пределами управляемой организацией среды ИКТ; а также неисправностью или небрежным обслуживанием систем. Выше перечислены, вероятно, наиболее распространенные формы угроз, с которыми организации сталкиваются каждый день. Таким образом, очевидна настоятельная необходимость наделения пользователей возможностями играть активную роль в повышении киберустойчивости организации.

97. **Цифровая грамотность — это не подлежащая обсуждению отправная точка.** В качестве предварительного условия для развития понимания того, как собственная практика кибербезопасности влияет на организацию, базовая цифровая грамотность каждого работника служит не подлежащей обсуждению отправной точкой. Возможность работать в цифровой среде больше не является необязательной для любого человека, каким-либо образом связанного с Организацией Объединенных Наций и ее работой в XXI веке. Комфортное использование стандартного электронного оборудования и приложений должно быть данностью для абсолютно каждого пользователя цифровой инфраструктуры организации, будь то сотрудники, аффилированный персонал, эксперты в командировках, делегаты конференций или любое другое лицо, подключающееся к внутренним киберресурсам или пользующееся ими. Только после выполнения этого фундаментального требования можно далее напомнить сотрудникам о том, что сохранение конфиденциальности, целостности и доступности информации и ресурсов организации — неотъемлемая часть работы и обязанностей каждого. Однако более сложный скачок может заключаться в переходе от повышения осведомленности о правилах, обязанностях и средствах кибербезопасности и руководящих указаниях по здоровой киберпрактике к достижению прочного изменения поведения и сдвига в индивидуальном и коллективном подходе.

98. **Признание важности обучения.** Один из способов изменить менталитет в сторону признания киберрисков и выработки здорового отношения к кибербезопасности — продуманные программы обучения и повышения информированности. Этот момент подчеркивается в специальной литературе и в докладах комитетов по ревизии и надзору, адресованных высшему руководству нескольких организаций системы Организации Объединенных Наций. Есть некий парадокс: часто создаются обширные и многоуровневые технические механизмы защиты инфраструктуры и систем, однако способность всех сотрудников демонстрировать практические знания об их использовании и возможностях, по-видимому, отстает, по крайней мере, в некоторых организациях, как можно судить по беседам с сотрудниками. Чем надежнее система, тем больше риск переходит на пользователей, и среди них наибольший риск представляют пользователи с плохой кибергигиеной. Как указал Независимый консультативный комитет по ревизии Секретариата Организации Объединенных Наций, «недостаток информированности может привести к неблагоприятным последствиям для систем информационно-коммуникационных технологий, конфиденциальности и целостности информации»[22].

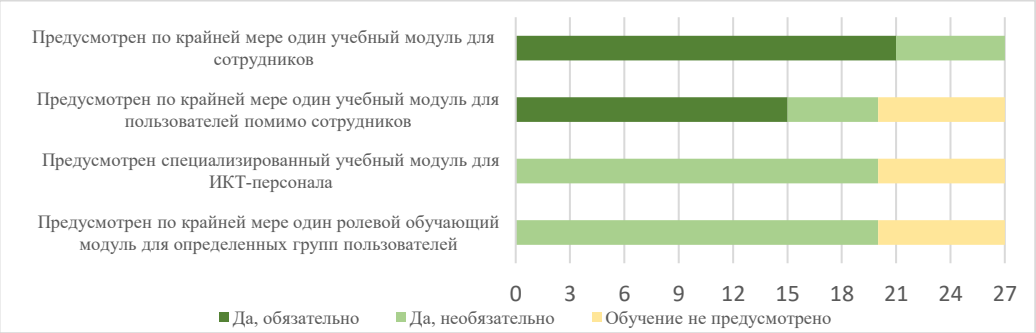
99. **Отображение возможностей обучения персонала показывает обнадеживающую ситуацию.** Сеть информационно-коммуникационных технологий на протяжении многих лет заявляла о важности обучения по вопросам

[22] A/73/304, п. 51.

информационной безопасности для системы Организации Объединенных Наций, и участвующие организации прилагали усилия для расширения организуемого ими обучения такого рода[23]. На диаграмме VII представлена информация, собранная по четырем категориям целевых аудиторий, подтверждающая проведение обязательных учебных занятий для сотрудников в большинстве организаций, а также показывающая, что в некоторых организациях такие занятия остаются необязательными. Такое обучение обычно посвящено правильному использованию учетных записей электронной почты для служебных, а не личных целей, рискам открытия вложений из неизвестных источников, рекомендациям по выбору паролей и работе с ними или безопасным действиям при работе с внешними сайтами. В последние годы комитеты по аудиту и надзору обращают внимание участвующих организаций на необходимость строже следить за прохождением обязательных учебных курсов, что в принципе является позитивным событием. Однако инспекторы хотели бы подчеркнуть, что прохождение обязательной подготовки само по себе редко служит содержательным показателем осведомленности и не обеспечивает достаточной уверенности в достижении реальных изменений в поведении. Более содержательным, при всех вероятных сложностях с его проведением и анализом, может быть сопоставление числа пользователей, совершающих нежелательные действия (такие, как нажатие на ссылку или вложение в фишинговом письме) за данный период времени, особенно до и после проведения учеб или мероприятий по повышению информированности. Некоторые полезные наработки, связанные с обязательным обучением, включают установление крайнего срока для новых сотрудников, позволяющего ограничить временное окно повышенного риска из-за неосведомленности, а также требование ежегодного прохождения сотрудниками повторных курсов для поддержания эффекта обучения с течением времени.

Диаграмма VII

Обучение в области информационной безопасности в 2020 году, по учебным модулям и числу организаций — участниц Объединенной инспекционной группы



Источник: Вопросник ОИГ 2020 года.

100. **Необходимость особого внимания к другим категориям персонала и эпизодическим пользователям.** Около половины участвующих организаций также установили обязательность обучения в области информационной безопасности для других категорий персонала, в то время как остальные проводят такое обучение в виде дополнительного модуля или вообще не предоставляют таких возможностей. Внимание к категориям пользователей помимо сотрудников действительно имеет важнейшее значение. Пользователи таких категорий часто вынуждены из-за ограниченности ресурсов использовать свои личные устройства для входа в системы организации. Кроме того, эпизодические пользователи систем и инфраструктуры организации с меньшей вероятностью будут информированы об их правильном и безопасном использовании в соответствии с действующими правилами и практикой организации. Отсутствие действенных механизмов контроля соблюдения правил лицами, прямо не нанятыми организацией и таким образом находящимися за пределами ее полной дисциплинарной юрисдикции, может еще больше ослабить

[23] См., например, CEB/2011/3 и CEB/2018/HLCM/ICT/10.

стимулы и привести к еще более слабому соблюдению требований. Эти проблемы могут еще больше усугубиться в организациях, где в числе сотрудников велика доля консультантов, подрядчиков и краткосрочного персонала. **Инспекторы напоминают, что инициативы по обучению и повышению осведомленности должны охватывать весь персонал. Угрозы не делают различий между разными категориями пользователей. Поэтому инспекторы предлагают исполнительным главам тех организаций, которые не сделали эти модули обязательными, принять соответствующие меры.**

101. **Проблемы, связанные с обучением.** До сведения инспекторов был доведен ряд проблем, с которыми сталкиваются участвующие организации, способных повлиять на осуществление результативной программы обучения в области кибербезопасности. Несколько организаций указали на финансовые ограничения, устанавливающие пределы возможностей предоставления ими обучения или доступа к нему, и, что вызывает беспокойство, некоторые из них были вынуждены выбрать для обучения только определенные категории пользователей. Финансовые ограничения дополнительно усугубляются быстро меняющимся характером темы, что может приводить к быстрому устареванию содержания курса, требуя обновления и дополнения, часто со значительными затратами. Другая проблема заключается в усталости пользователей от обучения, что может повлиять на эффективность программы. Высокая текучесть кадров и отсутствие контроля над некоторыми категориями персонала привносят дополнительные сложности. Организации, имеющие отделения на местах, могут сталкиваться со своими трудностями, что касается и любых других возможностей обучения. Однако этот аспект не может быть полностью изучен в рамках настоящего обзора. Наконец, сотрудники кибербезопасности отметили, что непрохождение обязательного обучения, как правило, не влечет за собой последствий, и связали возможную неэффективность многих программ обучения с отсутствием санкций, из-за которого даже обязательное обучение де-факто становится необязательным. **Для обеспечения более четкого контроля инспекторы предлагают исполнительным главам рассмотреть возможность установления официальной связи между завершением обучения по вопросам информационной безопасности и другими процедурами визирования в организации.** Это может включать привязку разрешения службы безопасности, необходимого для направления на работу на местах, и предоставление или продление доступа к системе ИКТ при условии подтверждения полученного обучения, включая курсы повторного обучения. Прецедент такого подхода уже существует в сфере соображений физической безопасности перед служебной командировкой, когда разрешение на такую поездку зависит от прохождения базовой подготовки по вопросам безопасности на местах, без которой в разрешении на поездку будет отказано.

102. **Инициативы по повышению осведомленности в системе Организации Объединенных Наций.** В системе Организации Объединенных Наций осуществляется целый ряд инициатив по повышению осведомленности о рисках для кибербезопасности и рекомендуемых мерах. Примером может служить октябрьская неделя информационной безопасности — инициатива, к которой присоединились несколько организаций по всему миру, в рамках которой проводятся интерактивные сессии, игры и информационные сессии. Программы Международной организации труда (МОТ) и ВОИС были названы особенно новаторскими и эффективными, а некоторые из них были признаны таковыми в контексте внешнего аудита. Другие идеи, которые представляют интерес, включают проведение мероприятий по повышению осведомленности о киберрисках, влияющих на частную сферу (например, о рисках, с которыми сталкиваются дети, или семейные фотографии, сделанные с целью получения выкупа), в надежде, что это вызовет больший интерес и что полученные сведения естественным образом окажутся востребованными и в профессиональной сфере на работе. Некоторые организации предусматривают очные вводные занятия для новых сотрудников, проводимые главным специалистом по информационной безопасности, в то время как другие закрепляют предоставленное обучение, распространяя короткие видеообращения среди сотрудников, ставших жертвами кибератаки. Имитационные фишинговые кампании являются одними из

самых популярных средств повышения осведомленности и, как сообщается, приносят результаты (вставка 5).

Вставка 5
Имитация фишинговых кампаний дает результаты

Под фишингом понимается отправка мошеннических электронных писем, якобы из надежного источника, чтобы выведать у людей конфиденциальную информацию. Затем злоумышленники используют такую информацию для получения несанкционированного доступа к системам организации в целях хищения средств организацию или другими злонамеренными мотивами.

Имитационные фишинговые кампании моделируют реальные приемы хакеров и помогают определить пользователей, которых легче обманом вынудить нажать на вредоносные ссылки или открыть зараженные вложения. Эти имитации также используются для проверки знаний, полученных в процессе обучения. Для их максимальной отдачи они должны дополняться поддержкой пользователей, например, назначением конкретного контактного лица и установлением простых и широко известных процедур для сообщения сотрудниками о подозрительных сообщениях. Так, некоторые участвующие организации предусмотрели возможность направления сообщения о фишинговых сообщениях путем нажатия кнопки непосредственно в приложении для обмена электронными сообщениями, используемом сотрудниками.

Цифры, предоставленные инспекторам, указывают на полезность таких имитаций фишинговых кампаний, поскольку сотрудники информационной безопасности обычно фиксируют снижение доли пользователей, открывающих подозрительные сообщения и вложения, в результате ряда таких занятий. Для общего сведения, по словам некоторых сотрудников кибербезопасности, обычно приемлемая доля внутренних пользователей, не соблюдающих правила среди всех пользователей, составляет около 5 % от общей численности персонала.

Имитации фишинговых кампаний часто проводятся в рамках более широких усилий по тестированию защищенности от проникновения. Такие имитации попыток взлома состоят из серии практических тренировок для выявления уязвимостей сетей, систем и людских ресурсов организации, измерения степени соблюдения правил и процедур, а также оценки эффективности защиты и процедур восстановления.

103. **Переход от учебных модулей к последовательной программе повышения осведомленности.** Вместо того, чтобы и далее предлагать каждому отдельные модули, не связанные стратегическим видением, **инспекторы рекомендуют организациям стремиться к разработке комплексной программы обучения и повышения осведомленности с четкими целями, определенными для каждой категории заинтересованных лиц с учетом рисков, которые могут быть связаны с ними для организации.** Следуя такой модели, организации смогут отказаться от статистики прохождения обучения как показателей соблюдения правил и вместо этого использовать обучение в качестве упреждающего инструмента для изменения внутренней культуры кибербезопасности. В идеале программа должна быть реализована с использованием инновационных методов обучения, сочетающих несколько подходов и приемов, учитывающих специфику каждой аудитории. Чтобы усилить чувство заинтересованности и способствовать лучшему усвоению знаний в этой области, организации могли бы также рассмотреть вопрос о создании системы взаимной поддержки и выявлении во всех подразделениях сотрудников, которые могут быть обучены в качестве координаторов программы, предоставляя необходимую практическую помощь коллегам.

I. Оптимизация выделения финансовых ресурсов на цели кибербезопасности

Оценка текущего объема ресурсов, выделяемых на кибербезопасность

104. **Ресурсы кибербезопасности, имеющиеся внутри системы Организации Объединенных Наций, как правило, меньше, чем внешние, но их трудно определить количественно.** Почти обычным явлением является утверждение, что организации системы Организации Объединенных Наций имеют в своем распоряжении меньше ресурсов, которые можно выделить на ИКТ в целом и на кибербезопасность в частности, по сравнению с организациями сопоставимого размера как в государственном, так и в частном секторе. Однако количественно оценить разрыв как в абсолютном, так и в относительном выражении сложно. Например, было подсчитано, что «менее 1 % расходов Организации Объединенных Наций приходится на ИКТ, и менее 1 % этой суммы зарезервировано на информационную безопасность, по сравнению со средним показателем в отрасли около 7 %»[24]. Стремясь предоставить основанный на фактах моментальный снимок ситуации, ОИГ провела опрос участвующих организаций по вопросу выделения ресурсов как на ИКТ, так и на кибербезопасность. Возможно, неудивительно, что инспекторы пришли к такому же выводу, который был указан в материалах заседаний симпозиума Специальной группы по информационной безопасности 2018 года: дать точные цифры по системе в целом по-прежнему невозможно.

105. **Сложность и полезность оценки расходов на кибербезопасность.** Несколько факторов затрудняют оценку ресурсов системы кибербезопасности. Затраты на кибербезопасность (вставка 6) обычно не выделяются в отдельную статью бюджета или категорию расходов. Финансирование, связанное с кибербезопасностью, может проходить по одной или нескольким статьям бюджета (например, расходы на основную деятельность, затраты на персонал или затраты на инфраструктуру или оборудование) или тематическим областям (например, в рамках ИКТ или за их пределами). Сложность поиска информации о ресурсах кибербезопасности и размере расходов в бюджетных документах и финансовых отчетах еще больше усугубляется разнообразием бюджетных структур, что находит отражение в одновременном составлении регулярных бюджетов и бюджетов добровольных (внебюджетных) взносов, некоторые из которых могут включать специальные счета капитальных вложений, используемые для крупномасштабных инфраструктурных проектов организации. Некоторые организации также различают (разовые) инвестиционные затраты и (текущие) расходы на основную деятельность, добавляя нюансы к общей картине. В одной организации было обнаружено, что большая часть ресурсов ИКТ сведена в программные бюджеты подразделений, эксплуатирующих системы ИКТ. На этом фоне сколь-нибудь уверенная оценка имеющихся общих ресурсов кибербезопасности практически невозможна. В любом случае это несоразмерно сложно по сравнению с полезностью: объем ресурсов организации, выделенных на кибербезопасность, лишь в ограниченной мере указывает на степень обеспечиваемой защиты.

Вставка 6
Затраты на кибербезопасность

- **Прямые затраты.** Очевидные (прямые) затраты на кибербезопасность варьируются от расходов на персонал (сотрудники и подрядчики) и расходов, связанных с инфраструктурой, таких как покупка оборудования и ПО (инвестиционные и эксплуатационные расходы и лицензионные выплаты), до услуг (например, подписка на аналитику угроз для безопасности и услуги, предоставляемые коммерческими поставщиками или Международным вычислительным центром Организации Объединенных Наций). Структура таких

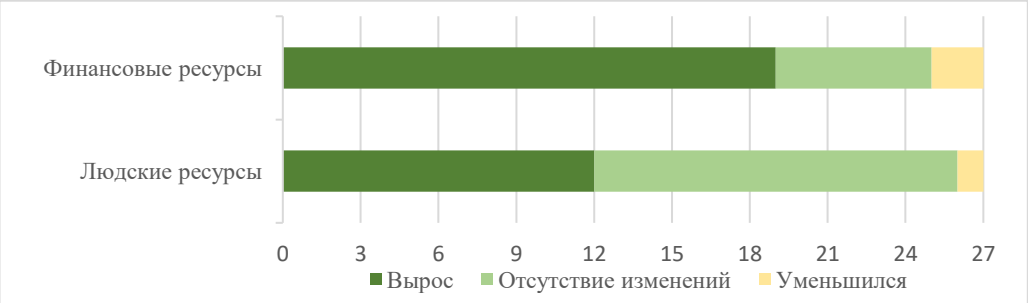
[24] CEB/2018/HLCM/ICT/4.

затрат может быть разной и отражает выбор каждой организации в отношении баланса собственного потенциала и внешнего подряда.

- **Косвенные расходы.** Кроме того, при определении стоимости кибербезопасности следует учитывать и другие (косвенные) затраты. Так, значительные финансовые последствия, как правило, связаны с мерами, принятыми для устранения ущерба после инцидента, включая разовое привлечение ресурсов для восстановления нарушенных систем, устранение недавно обнаруженных уязвимостей, снижение работоспособности при простое систем, обучение сотрудников по вопросам предотвращения несанкционированного доступа и реагированию на него, а также поддержание имеющегося специального потенциала (как кадрового, так и технического) на уровне предъявляемых требований.

106. **Недавняя тенденция: рост финансирования при сохранении ресурсных ограничений.** Инспекторы отмечают, что большинство участвующих организаций сообщили о росте ресурсов, выделяемых на кибербезопасность в последние годы (диаграмма VIII). На первый взгляд, это может показаться многообещающей тенденцией. Однако, как видно из диаграммы, сообщаемое увеличение финансовых ресурсов, по всей видимости, не привело автоматически к увеличению кадрового потенциала. Наоборот, подавляющее большинство участвующих организаций отметили, что нынешний уровень выделяемых ресурсов по-прежнему не позволяет создать эффективную структуру кибербезопасности, при этом одна организация даже сообщила, что затраты на ее ограждение и защиту от нарастающих киберугроз за два последних двухгодичных периода утроились. Согласно оценкам самих организаций, ограниченность ресурсов наиболее серьезно повлияла на кадровый потенциал и наличие своих специалистов, а также на возможности необходимых инвестиций в инфраструктуру ИКТ и замены устаревших приложений. Кроме того, в тех организациях, которые работают в условиях жестких ресурсных ограничений или нулевого бюджетного роста, ресурсы, вновь выделенные на кибербезопасность, могут быть получены в результате перераспределения, возможно, за счет других вложений, в основном в ИКТ, хотя и не только в них. Поскольку в долгосрочной перспективе такая тенденция может оказаться неустойчивой, инспекторы обеспокоены тем, что выделяемые ресурсы, даже если они были увеличены, возможно, не росли такими же темпами, что техническая изощренность злоумышленников и повсеместное распространение ИКТ в работе организаций системы Организации Объединенных Наций. Как правильно отмечалось в Специальной группе по информационной безопасности, растущая зависимость от информационных технологий не сопровождается соразмерным увеличением ресурсов информационной безопасности[25].

Диаграмма VIII
Эволюция ресурсов кибербезопасности по данным организаций — участниц ОИГ (2015–2020 годы)



Источник: Вопросник ОИГ 2020 года.

[25] Ibid.

107. **Источники финансирования.** Согласно собранной информации, в большинстве участвующих организаций средства для кибербезопасности в основном поступают из их регулярного бюджета. Некоторые из них используют одновременно бюджетное и внебюджетное финансирование, в то время как очень немногие используют только внебюджетное финансирование. Относительная предсказуемость финансирования из регулярного бюджета может способствовать устойчивости потенциала кибербезопасности, но этот подход требует стратегического планирования для обеспечения того, чтобы необходимые средства поступали тогда, когда они необходимы. В то же время внебюджетное финансирование способно обеспечить бо́льшую гибкость и может быть более привлекательным для доноров, желающих выделить такие средства для кибербезопасности. У небольшого числа организаций есть специальный фонд: либо фонд, предназначенный для инфраструктуры ИКТ (ВОЗ), либо фонд, который можно привлечь для крупных корпоративных проектов (ВОИС и МАГАТЭ). Как упоминалось в связи с долгосрочными дорожными картами совершенствования системы кибербезопасности организаций, инвестиции в этой области, как правило, по своему характеру охватывают многолетний период. Таким образом, текущие бюджетные циклы могут быть слишком короткими, не позволяя укорениться долгосрочным стратегическим соображениям, и при этом недостаточно гибкими, не позволяя направить средства для удовлетворения разовых краткосрочных требований, которые могут возникнуть в технологической сфере и в столь быстро меняющемся ландшафте угроз, как ландшафт киберугроз. Специальные фонды могут восполнить этот пробел при условии, что их принципы управления и их условия, одобренные директивными и руководящими органами, позволяют им это делать.

На пути к оптимизации инвестиций в кибербезопасность

108. **Необходимость экономического обоснования запросов о выделении ресурсов к руководящим органам.** Очевидно, что организации не могут ожидать, что их запросы о выделении ресурсов, направляемые руководящим органам, будут удовлетворяться в отсутствие надлежащего обоснования приоритета инвестиций в кибербезопасность по отношению к другим расходам организации. **В качестве отправной точки инспекторы рекомендуют строить запросы о выделении ресурсов на тщательной оценке рисков и экономическом обосновании, конкретно указывающем затраты, выгоды, риски и ожидаемую экономию и определяющем потенциальные финансовые последствия отказа от инвестиций.** Такой подход наиболее эффективен в сочетании с предлагаемым планом и графиком реализации, например в форме дорожной карты, как это аргументируется в другой части настоящего доклада, и в представлении отчетности о ходе реализации на регулярной основе. Инспекторы отметили, что, когда исполнительное руководство представляло убедительное экономическое обоснование с четкими целями и параметрами для улучшения и продемонстрировало важность инвестиций, руководящие органы, как правило, были более готовы поддержать эти планы выделением целевых ресурсов. В последние годы это имело место в ИКАО, МОТ, УВКБ, ВОИС и других организациях, и такая практика обнадеживает, поскольку вполне вероятно, что растущая изощренность киберугроз будет и дальше требовать больше ресурсов, а не меньше.

109. **Расходы на кибербезопасность можно и нужно оптимизировать.** Само собой разумеется, что мощная и хорошо защищенная система кибербезопасности имеет свою цену, и если организации системы Организации Объединенных Наций серьезно относятся к защите своей информации, систем и цифровых ресурсов, то они должны выделять необходимые средства для своих систем кибербезопасности. Попытки определить необходимый уровень ресурсного обеспечения кибербезопасности в соотношении с бюджетами ИКТ организаций не дали значимых результатов. Идею определения необходимых ресурсов в денежном выражении не следует фетишизировать, поскольку одни деньги не решат проблему. «Гартнер» поставил проблему прямо: сумма, потраченная на кибербезопасность, не отражает уровня

защиты[26]. Более важным, чем вопрос о том, сколько следует потратить на кибербезопасность, является вопрос о том, где следует вложить ресурсы, чтобы получить наибольшую отдачу. Ответы на анкеты ОИГ указывают на непоследовательность подходов к определению приоритетов расходов на кибербезопасность, что увеличивает риск неэффективности использования и без того скудных ресурсов. Весьма убедительный, хотя и в некоторой степени сложный и требующий активной адаптации вариант определения необходимого размера инвестиций в кибербезопасность — следовать строгой методике, такой как Шервудская прикладная архитектура безопасности предприятия (или эквивалентной методике), которая основана на концепции двунаправленной прослеживаемости. Иными словами, архитектура безопасности предприятия в соответствии с этой методикой определяется таким образом, что каждому бизнес-требованию соответствует, по крайней мере, одно средство обеспечения безопасности и каждому средству обеспечения безопасности может соответствовать обозначенное бизнес-требование обеспечения безопасности[27]. ВОИС уже использует эту методику, которая также обсуждалась в контексте Специальной группы по информационной безопасности и**, по мнению инспекторов, заслуживает дальнейшего изучения в качестве средства достижения того, чтобы инвестиции в кибербезопасность прочно основывались на требованиях деятельности организации и разумных методах управления рисками и были увязаны с ними, что позволяет избежать чрезмерного инвестирования и недофинансирования ключевой функции обеспечения бесперебойности деятельности.**

Вставка 7
Решения с открытым исходным кодом могут дать экономически эффективные альтернативы

Программное обеспечение с открытым исходным кодом как модель разработки и распространения ПО стала неотъемлемой частью отрасли ИКТ. Некоторые средства, основанные на ПО с открытым исходным кодом, широко используются в области кибербезопасности и затрагивают такие аспекты, как обмен данными об угрозах, управление идентификацией и доступом, сетевой анализ, обнаружение и предотвращение вторжений, реагирование на инциденты и криминалистика. Некоторые примеры ПО с открытым исходным кодом даже известны как ведущие ресурсы в своих соответствующих категориях.

Хотя ответы на анкету ОИГ указывают на то, что некоторые участвующие организации уже дополняют свои приобретенные у коммерческих поставщиков и разработанные своими силами решения ПО с открытым исходным кодом, может существовать возможность более широкого использования таких вариантов организациями системы Организации Объединенных Наций. Они могут давать подходящие решения, особенно для организаций, работающих в условиях нехватки ресурсов.

Как и любой коммерческий продукт, решения с открытым исходным кодом следует оценивать по их конкретным достоинствам, но у них есть определенные общие преимущества, которые часто связаны с четким обслуживанием программных продуктов с открытым исходным кодом, такие как прозрачность, безопасность, более низкая стоимость лицензий и выплат, использование открытых стандартов и ограниченная опасность привязки по поставщику.

[26] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.
[27] Подробнее о Шервудской прикладной архитектуре безопасности предприятия см. URL: https://sabsa.org/sabsa-executive-summary.

Хотя использование ПО с открытым исходным кодом обычно не связано с затратами на лицензирование, это не означает, что оно полностью бесплатно. Его установка, настройка и обслуживание, а также соответствующая степень овладения им требуют затрат времени сотрудников и, следовательно, расходов. Полная стоимость владения такими платформами может быть неочевидна для организаций с ограниченными техническими ресурсами и опытом внедрения таких приложений, хотя это соображение часто касается — в той или иной степени — и коммерческих продуктов.

Организациям не следует мыслить дихотомиями — чисто коммерческая модель или модель только с открытым кодом. Имеются продукты, основанные на гибридной модели, нацеленной на объединение лучшего из обеих моделей, а именно свободы и прозрачности ПО с открытым исходным кодом и организованной поддержки, обеспечиваемой подвижными поставщиками. Другой вариант — использовать как коммерческие средства, так и ПО с открытым исходным кодом для разных функций и целей внутри организации.

J. Инвестирование в занимающихся этим вопросом специалистов

Подразделение информационной безопасности имеется не у всех участвующих организаций

110. **Обязанности, связанные с кибербезопасностью, выходят за рамки технических познаний.** Большинство участвующих организаций вложили средства в привлечение специалистов, занимающихся различными аспектами кибербезопасности, иногда под руководством специально назначенного главного сотрудника по информационной безопасности. Основные аспекты, входящие в сферу ответственности соответствующего подразделения, включают разработку средств защиты на рабочем уровне, с одной стороны, и руководство на стратегическом уровне — с другой, с целью достижения целей защиты кибербезопасности, как это отражено в определении, упомянутом в настоящем докладе. Таким образом, объем этих функций выходит за рамки цифровой сферы и не ограничивается предоставлением технических ноу-хау. Он включает разнообразные задачи, такие как разработка и информационное сопровождение регулирующих норм организации (разработки политики и информационное сопровождение); консультирование по вопросам выявления рисков и управления ими (управление рисками); взаимодействие с подразделениями при проведении оценки рисков и анализа воздействия на деятельность (координационная и аналитическая роль); расследование серьезных нарушений (возможности расследования и анализа); представление рекомендаций, а также принятие необходимых мер по усилению защиты (практические и технические специальные знания)[28]. Это описание задач подразумевает, что эти функции содержат управленческий аспект, как в среде ИКТ, так и за ее пределами, и требуют работы в тесном сотрудничестве с широким кругом заинтересованных сторон, особенно с подразделениями организаций. Таким образом, делегированные главному сотруднику по информационной безопасности (и экспертам по кибербезопасности в более общем плане) полномочия по информационному сопровождению и побуждению к действиям в масштабах организации приобретают первостепенное значение.

111. **Различия во внутреннем потенциале.** Как показало исследование, проведенное ОИГ, по крайней мере 16 участвующих организаций создали специализированный и предназначенный для данной цели кадровый потенциал, начиная от одного эксперта по информационной безопасности, иногда совмещающего эти задачи с другими, до целого организационного подразделения, возглавляемого главным сотрудником по информационной безопасности, обычно класса С4 или С5 (приложение V). Наоборот, в 10 участвующих организациях задачи кибербезопасности выполняются в основном специалистами по ИКТ в дополнение к другим их обязанностям. Из-за технической сложности этой области, которая

[28] См. SFIA Foundation, *Skills Framework for the Information Age (SFIA) 7*, 2018.

постоянно развивается и требует значительной степени специализации, которую сложно и дорого поддерживать на постоянной основе на уровне предъявляемых требований, очень часто привлекаются специалисты со стороны, включая временных сотрудников, таких как консультанты и подрядчики, и подписку на услуги коммерческих поставщиков или Международного вычислительного центра Организации Объединенных Наций. Некоторые собеседники отметили, что глобальная нехватка опытных практиков в области кибербезопасности является одной из самых больших проблем, с которыми сталкиваются организации системы Организации Объединенных Наций при создании, поддержании и курировании своих программ кибербезопасности. Чтобы предоставить альтернативу организациям, которые не в состоянии немедленно выделить специальное направление, инспекторы хотели бы подчеркнуть, что Международный вычислительный центр Организации Объединенных Наций предлагает услугу «управление безопасностью», которую иногда также называют «главный сотрудник по информационной безопасности как услуга», на которую в настоящее время подписаны шесть участвующих организаций, а еще четыре организации пользовались этой услугой в прошлом. **Инспекторы считают, что организациям системы Организации Объединенных Наций необходимо удовлетворять будущие потребности в экспертных знаниях в области кибербезопасности путем надлежащего планирования людских ресурсов, особенно с учетом того, что знания, навыки и способности для устранения рисков и проблем кибербезопасности имеют конкретный характер и имеющих их сотрудников может быть непросто привлечь и удержать.**

112. **Стоит подумать об инвестировании в специальный потенциал.** При том что структуры организации в идеале должны отражать ее размеры и конкретные требования и основываться на проведенной оценке рисков и киберсреды, в которой работает организация, реальность такова, что другие факторы могут быть более важными. В частности, различия во внутренней структуре, отмеченные инспекторами в участвующих организациях, могут указывать скорее на ограничения, с которыми сталкивается каждая из них, а не на целенаправленный или стратегический выбор. Так, в четырех участвующих организациях направление кибербезопасности считалось в лучшем случае зарождающимся, что косвенно может поставить под угрозу всю систему. **Инспекторы считают, что наличие в каждой организации занимающимися вопросами кибербезопасности специалистов способствует улучшению состояния кибербезопасности не только в этой организации, но и в системе в целом, и поэтому такие затраты оправданы.** Как и в случае с другими направлениями, связанными с основной деятельностью организаций, создание прочного внутреннего кадрового потенциала для защиты информации и киберресурсов там, где это возможно, обычно предпочтительнее, чем раз за разом привлекать временные ресурсы, не в последнюю очередь из-за дополнительных рисков, связанных с их использованием и ограниченными возможностями контроля организаций по сравнению с штатными сотрудниками (пункт 100). Кроме того, **введение штатной должности главного сотрудника по информационной безопасности для руководства и управления такими специалистами может обеспечить необходимую направленность и согласованность подхода и, по мнению инспекторов, будет способствовать повышению киберустойчивости данной организации.**

113. **Отсутствие общепринятой организационной схемы, определяющей подразделение, которому поручены функции кибербезопасности.** Оптимальное место подразделения, на которое возложены функции обеспечения кибербезопасности, в организационной структуре — это вопрос, который обсуждался в системе Организации Объединенных Наций и за ее пределами, и на который нет окончательного универсально применимого ответа. Международные стандарты не дают авторитетных указаний и оставляют за каждой организацией право определять, какому именно подразделению должны быть поручены функции кибербезопасности, в соответствии со своими задачами и архитектурой. В организациях системы Организации Объединенных Наций в большинстве случаев эти функции возложены на подразделение ИКТ, что обычно отражается в прямой подчиненности начальнику подразделения или аналогичному сотруднику. Такую наиболее распространенную

схему можно рассматривать как наследие прошлого, но она отражает ту реальность, что кибербезопасность естественным образом тяготеет к ИКТ в силу технических знаний и опыта, необходимых для управления соответствующими информационными системами и другой инфраструктурой защиты. Кроме того, подразделение ИКТ часто разрабатывает и реализует меры оперативного реагирования на кибератаки, и разделение обоих направлений может привести к снижению эффективности.

114. **Согласование расходящихся организационных приоритетов по направлениям ИКТ и кибербезопасности.** Несмотря на сказанное выше, подчинение сотрудника или группы, отвечающей за кибербезопасность, руководителю подразделения ИКТ может создать несоответствие между основными задачами каждого такого сотрудника, при этом управление рисками и информационная безопасность составляют основную задачу главного сотрудника по информационной безопасности в отличие от вопросов практической деятельности и экономической эффективности, а также оперативности обслуживания, которыми ведает руководитель подразделения ИКТ. Потенциальный конфликт интересов очевиден, но его нелегко разрешить. Узкоспециальный подход к кибербезопасности (например, ожидаемый от специалистов по ИКТ) может многократно усилить негативное влияние на ее обеспечение в дальнейшем, когда киберриски, которые могли быть отброшены ранее, начнут материализоваться. В то же время чрезмерное избегание риска (например, ассоциируемое со специалистами по кибербезопасности) может чрезмерно парализовать оперативную гибкость и помешать выполнению мандата другими способами. Согласование различных целей организации и устранение противоречий между ними, в том числе в разрезе ресурсов, — часть повседневных задач каждого руководителя, и исполнительное руководство лучше всего подходит для достижения баланса в этом отношении.

115. **Расширение возможностей подразделения кибербезопасности.** Независимо от того, какому подразделению организации поручено обеспечение кибербезопасности, **инспекторы подчеркивают, что важно обеспечить, чтобы соображения кибербезопасности могли без ограничений высказываться и учитываться ответственными лицами, принимающими решения.** Эти задачи должны решаться там, где соответствующие сотрудники могут самостоятельно выходить на исполнительное руководство и вносить реальный вклад в деятельность других систем организации, таких как общеорганизационное управление рисками, управление информацией и знаниями, физическая охрана и безопасность, — мысль, которая проводится на протяжении всего доклада. Залогом этого служит наличие мощного внутреннего механизма управления с участием многих заинтересованных сторон, включая все соответствующие подразделения. Некоторые хорошо проработанные примеры таких многосторонних и многоуровневых механизмов управления были предоставлены ВОИС и ИКАО.

116. **Специализированное обучение.** Независимо от того, кто отвечает за кибербезопасность в организации, и от того, поручены ли эти задачи одному сотруднику или группе сотрудников, специально занимающихся ими, или нескольким сотрудникам и подразделениям, выполняющим и другие функции, важно, чтобы специализированное обучение оставалось доступным для всех сотрудников ИКТ, ведающих вопросами безопасности, чтобы они могли постоянно повышать свой профессиональный уровень. Такое обучение специалистов по ИКТ, например разработчиков или системных администраторов, как сообщается, уже ведется в большинстве организаций и заслуживает дальнейшего поощрения (диаграмма VII). Действенная программа обучения кибербезопасности и, при необходимости, процесс присвоения квалификации отобранным сотрудникам по ИКТ в идеале должны быть центральным элементом плана работы их подразделения и обеспечиваться надежным бюджетом. Без выделения на цели непрерывного повышения квалификации определенных средств персоналу ИКТ остается поддерживать свои профессиональные знания по собственной инициативе или путем своего участия в профессиональных сообществах. Этот подход слишком сильно зависит от личного отношения специалиста, и вряд ли на него можно рассчитывать в каждом случае. Инспекторы приветствуют намерения нескольких организаций усилить эту область, но отмечают, что даже в тех случаях, когда уровень ресурсов позволяет предоставлять такую

специализированную подготовку, в большинстве случаев она проводится на разовой основе, не ставит долгосрочных целей обучения и не строится на системном подходе. В частности, там, где для обеспечения кибербезопасности не выделены сотрудники, специально занимающиеся этим на постоянной основе, тем более важны надлежащие возможности обучения сотрудников, которым поручено соответствующее направление.

Центр обеспечения безопасности как узловое звено реагирования в области кибербезопасности

117. **Основные функции центра обеспечения безопасности.** Центр обеспечения безопасности — подразделение организации, которое занимается повседневным обеспечением кибербезопасности. Хотя между его различными воплощениями неизбежны различия, самый широкий мандат возлагает на центр ответственность за контроль безопасности организации путем предотвращения, обнаружения и анализа киберинцидентов и реагирования на них. Эксперты по кибербезопасности часто говорят, что центр обеспечения безопасности, в котором взаимодействуют люди, технологии и процессы, служит узловым звеном сбора, сопоставления и анализа потоков информации из различных источников в реальном времени. Внутренняя информация, собираемая и обрабатываемая таким центром, может включать данные из таких источников, как сетевые устройства, серверы и размещенные приложения, настольные компьютеры и мобильные устройства, системы физической безопасности и специальные устройства защиты. Центр обеспечения безопасности также собирает и обрабатывает аналитические данные об угрозах из внешних источников, обычно обращаясь к данным из открытых источников (включая общедоступную информацию от государств), а также коммерческой аналитике угроз, которая сопоставляется с внутренними данными и анализируется на предмет новых угроз. Учитывая сложность задач и необходимость специалистов разного профиля, создание и поддержание в полностью рабочем состоянии центра обеспечения безопасности может быть сложным и затратным. Необходим ли такой центр и, если он необходим, то должен ли он быть создан внутри организации или обеспечиваться сторонней структурой — это вопросы, на которые каждая организация должна ответить в свете своих собственных требований.

118. **Собственные, подрядные или гибридные решения для центров обеспечения безопасности: разнообразные варианты, наблюдаемые в организациях.** У участвующих организаций имеются разные мнения о преимуществах и недостатках внутренних решений по сравнению с внешними, на что указывает разнообразие механизмов и методов, выявленных инспекторами в ходе обзора. Некоторые организации используют виртуальный или распределенный центр обеспечения безопасности в том смысле, что некоторые из его функций распределены между децентрализованным пулом кадровых ресурсов. Ряд организаций приняли решение создать свой внутренний центр, в то время как другие используют внешний центр, размещенный у коммерческих поставщиков, или совместно с другими организациями используют услуги центра, обеспечиваемые Международным вычислительным центром Организации Объединенных Наций, которые могут дополняться собственным подразделением. Организации, использующие такие гибридные решения, в некоторых случаях проводят различие между стратегическими и надзорными функциями, которые остаются за организацией, и текущим контролем, особенно в случае круглосуточного («24/7») контроля, который передается внешним поставщикам. Некоторые из них даже используют более одного центра обеспечения безопасности, что позволяет им отделить определенную часть наиболее конфиденциальных данных от массивов данных, управление которыми доверено внешними структурам. Инспекторы отметили, что несколько участвующих организаций в настоящее время рассматривают вариант создания центра обеспечения безопасности.

119. **Рассматриваемые элементы организации центра обеспечения безопасности.** Аргументы в пользу создания внутреннего центра включают возможность быстрее реагировать на угрозы и уязвимости, а также лучше контролировать оконечные устройства, хотя и, конечно, при более высоких расходах.

Последнее достигается благодаря большей прямой видимости таких устройств и их состояния при возможности устранения уязвимостей оконечных устройств в реальном времени. Кроме того, создание внутреннего центра считается действенным способом централизации функций кибербезопасности, что, согласно широкому консенсусу среди специалистов, приводит к повышению общей киберустойчивости. Для многих организаций системы Организации Объединенных Наций расходы на собственный центр обеспечения безопасности могут быть запретительными, а получаемые положительные результаты могут не соответствовать профилю кибербезопасности таких организаций и связанным с ними требованиям защиты. Лишь немногие структуры Организации Объединенных Наций могут позволить себе полноценную программу кибербезопасности для самостоятельного противодействия угрозам и реагирования на них, опираясь только на собственный потенциал. Более того, даже если им удастся создать необходимые структуры, они все равно могут не получить находящуюся в постоянной оперативной готовности группу разносторонне подготовленных и обученных экспертов по кибербезопасности, способных реагировать на сложные кибератаки, которые, как правило, бывают нечастыми и разнообразными, что подразумевает некоторые изменения профиля необходимых специалистов. К тому же некоторые организации считают, что поддержание полноценного собственного потенциала для решения всех рабочих задач не позволит достичь уровня внешних специализированных поставщиков, которые к тому же имеют больше ресурсов для инвестирования в разработки и исследования, считающиеся совершенно необходимыми для динамичной области кибербезопасности. В то же время подчеркивалось, что, даже если организации выбирают внешний подряд, внутри организации требуется достаточный уровень внутреннего потенциала и представленность некоторых основных функций кибербезопасности, обладающих экспертными знаниями о внутренних рабочих процессах и способных служить действенным связующим звеном со сторонним поставщиком. В случаях, когда используются внешние центры обеспечения безопасности, контроль за поставщиками также становится ключевой задачей и должен обеспечиваться тщательной проверкой, соответствующими положениями о правовой защите в контрактах и недопущением зависимости от поставщика или привязки к нему. Некоторые из соображений в пользу или против передачи центра обеспечения безопасности на внешний подряд могут касаться и других решений о выборе между внутренними или внешними структурами обеспечения кибербезопасности и кратко изложены во вставке 8.

Вставка 8
Привлечение внешних поставщиков услуг центра обеспечения безопасности и других услуг кибербезопасности

Плюсы:

- Возможность привлечения разнообразных, современных и узкоспециализированных профессиональных знаний и средств
- Возможная экономия затрат
- Возможность увеличения или уменьшения масштаба в соответствии с постоянно меняющимся ландшафтом угроз и меняющимися требованиями к ресурсному обеспечению
- Предполагаемая нейтральность и беспристрастность

Минусы:

- Возможность зависимости от поставщика (привязки)
- Возможность трудностей с адаптацией стандартизированных услуг и решений к конкретным условиям, приводящих к неоптимальным и жестким решениям
- Повышенная зависимость от неизвестных или непроверенных сотрудников, находящихся под прямым контролем руководителей
- Возможность утечки конфиденциальных данных третьим лицам

- Ограниченная прозрачность в плане информирования об инцидентах
- Затраты

120. **Центр обеспечения безопасности улучшает согласованность реагирования в области кибербезопасности.** Каждой организации следует решить, стоит ли ей создать такой центр, проанализировав затраты и результаты с использованием таких параметров, как сложность ее системы ИКТ, число и характер критически важных ресурсов и управляемых процессов, а также общий объем потоков данных и, следовательно, периодичность угроз, которые могут указывать на разную степень необходимости постоянного контроля и защиты. Инспекторы хотели бы подчеркнуть, что один из важных аспектов официального центра обеспечения безопасности, независимо от его размера и ресурсов, — достигаемая благодаря ему нацеленность и согласованность текущего контроля и деятельности в организации. Даже очень небольшая группа, которой необходимо привлекать сотрудников по ИКТ других подразделений организации или внешних поставщиков, тем не менее, может выполнять важную роль по координации и синхронизации и повышать информированность в организации. **Поэтому инспекторы предлагают исполнительным главам рассмотреть вариант создания центра обеспечения безопасности или оптимизации имеющихся ресурсов в рамках эквивалентного механизма на основе критического анализа требований их организаций, а также внутренних и внешних возможностей, уже имеющихся в их распоряжении, и обеспечить, чтобы они могли исчерпывающим образом мотивировать свое решение создать центр обеспечения безопасности или не создавать его.**

K. Отражение общеорганизационных усилий по повышению киберустойчивости, включая отчетность

121. Степень, в которой элементы, описанные в настоящей главе, отражены в подходе организации к кибербезопасности, прямо влияет на ее способность выявлять, предотвращать и обнаруживать киберугрозы, а также реагировать на инциденты и устранять их последствия. Помня о том, что созданные механизмы могут быть результатом стратегического или практического выбора или продиктованы другими соображениями, исполнительным главам следует начать общеорганизационный обзор для изучения того, в какой степени каждый из этих элементов отражен в политике и практике их организаций.

122. Ожидается, что выполнение следующих рекомендаций повысит эффективность мер готовности и реагирования организаций системы Организации Объединенных Наций в области кибербезопасности.

Рекомендация 1

Исполнительным главам организаций системы Организации Объединенных Наций следует в первоочередном порядке и не позднее 2022 года подготовить всеобъемлющий доклад о своей системе кибербезопасности и представить его своим соответствующим директивным и руководящим органам при первой возможности, охватив элементы, способствующие повышению киберустойчивости, рассмотренной в настоящем докладе.

123. Выводы такого внутреннего обзора, включая выявленные сильные и слабые стороны и предложения о мерах по дальнейшему усилению киберустойчивости, следует представлять директивным и руководящим органам. По мнению инспекторов, после этого директивные и руководящие органы смогут дать содержательные стратегические указания высокого уровня на основе официально объявленной допустимой степени риска в области кибербезопасности и выделить ресурсы для достижения желаемого уровня защиты. Как указано выше, исполнительному руководству следует рассмотреть возможность регулярной отчетности по вопросам

кибербезопасности перед директивными и руководящими органами. Инспекторы признают, что в некоторой части информация, представленная в таком докладе, может быть конфиденциальной и, возможно, потребует соблюдения необходимых правил ее ограждения. **Поэтому исполнительному руководству рекомендуется проявлять максимальную осторожность при выборе формата и канала отчетности, обеспечивающих предоставление соответствующему директивному и руководящему органу необходимой информации, не ставя под угрозу защиту организации.**

Рекомендация 2

Директивным и руководящим органам организаций системы Организации Объединенных Наций следует по мере необходимости рассматривать доклады об элементах, способствующих повышению киберустойчивости, подготовленные исполнительными главами, и давать стратегические указания относительно дальнейших улучшений, которые должны быть достигнуты в их организациях.

IV. Кибербезопасность с общесистемной точки зрения

A. Кибербезопасность — общесистемный приоритет?

124. **Общесистемное сотрудничество в области кибербезопасности — давно заявленный приоритет.** Улучшение состояния кибербезопасности в системе Организации Объединенных Наций на протяжении многих лет объявляется приоритетной задачей как государствами-членами, так и руководством Организации Объединенных Наций на самом высоком уровне. Так, в 2008 году Генеральная Ассамблея призвала Генерального секретаря как председателя КСР способствовать более тесной координации и сотрудничеству между организациями системы Организации Объединенных Наций по всем вопросам, касающимся ИКТ, общеорганизационного планирования ресурсов, и в частности безопасности, послеаварийного восстановления и непрерывности деятельности[29]. В 2013 году Консультативный комитет по административным и бюджетным вопросам при рассмотрении доклада о ходе выполнения рекомендаций, касающихся повышения безопасности информации и систем во всем Секретариате, рекомендовал Генеральному секретарю продолжить общесистемное взаимодействие и изыскивать любые возможности дальнейшего сотрудничества и совместного использования решений информационной безопасности организациями системы Организации Объединенных Наций[30]. Недавно, в 2019 году, в рамках завершения дискуссии на уровне КСР сам Генеральный секретарь подчеркнул важность укрепления собственных возможностей системы Организации Объединенных Наций по защите от кибератак[31]. Главная посылка в этой связи заключается в том, что более широкое сотрудничество на общесистемном уровне, включая совместные подходы и общие практические решения, служит одним из ключевых факторов повышения уровня защиты системы в целом.

125. **Попытки совместного стратегического подхода.** Как уже отмечалось, организации системы Организации Объединенных Наций в основном сталкиваются с одними и теми же вызовами и угрозами в киберсреде, что подразумевает наличие потенциала для разработки совместного подхода к мерам реагирования. Поскольку безопасность системы зависит, по крайней мере частично, от безопасности отдельных ее членов с учетом их взаимосвязанности на различных уровнях, для этого также есть веская причина. Во время подготовки настоящего обзора несколько участвующих организаций призывали к разработке общей стратегии, осуществляемой при живом участии и отчетности учреждений как партнеров, выступающих согласованно и движимых общей целью достижения определенной степени зрелости всей системы на основе ряда минимальных критериев, которым должны соответствовать все. Призыв к выработке общесистемной стратегии кибербезопасности, которая должна способствовать созданию основы последовательной практики кибербезопасности во всей системе, имеется в материалах Сети информационно-коммуникационных технологий 2017 года[32]. Однако эта инициатива, похоже, не материализовалась и не получила развития в каком-либо осязаемом виде. Еще одна попытка продвижения согласованного подхода была связана с предложением ежегодно проводить обследование среди организаций на предмет их мер кибербезопасности, чтобы выработать внутренний эталон зрелости и лучше оценить общую подверженность системы риску. Несмотря на значительную подготовительную работу, которая включала два экспериментальных раунда обследования, проведенных среди примерно 20 организаций в 2018–2019 годах, тогда это предложение не нашло коллективной поддержки со стороны высшего руководства. Основными аргументами, выдвигаемыми при отказе от таких усилий по сопоставительному анализу, были, с одной стороны, разнообразие организационных структур и условий, ограничивающих ценность коллективной оценки, и, с другой стороны, ограниченная

[29] Резолюция 63/262 Генеральной Ассамблеи.
[30] A/68/7/Add.11, п. 6.
[31] CEB/2019/2, para. 39.
[32] CEB/2017/HLCM/ICT/9, pp. 7–8.

готовность организаций делиться своими внутренними оценками кибербезопасности за пределами своей организации, когда риски для кибербезопасности фактически приводились как главное препятствие для проведения даже обобщенной оценки. Мнения, высказанные в ходе бесед, указывают на то, что пандемия COVID-19 могла привести к изменению представлений и взглядов в отношении кибербезопасности и что предложения, ранее считавшиеся далекоидущими или нереалистичными, сегодня могут иметь больше шансов вызвать интерес и одобрение. В этой связи дискуссия о возможности применения эталонной модели зрелости, аналогичной модели, которая была недавно принята Форумом по управлению рисками КСР, по-видимому, возобновилась в контексте последнего межведомственного совещания экспертов по кибербезопасности.

126. **Коллективная ответственность за обеспечение минимального уровня защиты.** Стремление к полной общесистемной унификации, в частности на основе выводов, сделанных по результатам сопоставительной оценки зрелости организаций, действительно может быть чрезмерно далекоидущим и даже ненужным. Как отметил аналитический центр «Гартнер», попытка сопоставить организационные механизмы и меры кибербезопасности друг с другом может послужить основой выводов об относительной зрелости каждой организации, но не дает никаких надежных указаний об абсолютном уровне защиты какой-либо из них[33]. Однако репутационная, а также практическая взаимозависимость между организациями системы Организации Объединенных Наций влечет за собой их коллективную обязанность поднимать планку как можно выше для всех и помогать друг другу в ее достижении. Следует отметить, что именно те организации, которые обладают развитой структурой кибербезопасности и сильным внутренним или внешним потенциалом, больше всего поддерживали такие усилия. Это тонкая грань, но крайне важно, чтобы система находила правильный баланс между соответствующими требованиями участвующих организаций, существующими в них механизмами и общесистемным подходом к определению минимального стандарта, который должен быть достигнут всеми и в интересах всех. **По мнению инспекторов, определение базового уровня защиты и минимальных требований к ней для организаций системы Организации Объединенных Наций и, следовательно, для системы в целом остается значимой целью, к которой по-прежнему стоит стремиться.**

127. **Усилия по созданию общей структуры на практическом уровне.** Вопрос об объединенной общесистемной структуре по предотвращению и обнаружению киберугроз и атак и реагированию на них неоднократно обсуждался на различных уровнях. Почти 10 лет назад Сеть информационно-коммуникационных технологий опубликовала план создания группы Организации Объединенных Наций по реагированию на компьютерные инциденты[34]. Эта инициатива не была реализована, поскольку в то время не могло быть достигнуто договоренности о модели ее финансирования. Позднее Специальная группа по информационной безопасности возобновила свою работу по оценке возможности создания общего центра обеспечения безопасности для подразделений Организации Объединенных Наций, однако в ходе обсуждения между ее членами было выявлено множество нерешенных проблем (распределение расходов, согласование с различными ранее созданными структурами, договоренность об ожидаемом объеме и приоритетах поддержки в случае широкомасштабной атаки и т. п.). Эти усилия основывались на ожидании того, что общесистемная структура реагирования на инциденты создаст потенциал значительного повышения эффективности, а также обеспечит усиление защиты, особенно для организаций, которые не могут позволить себе иметь специальную структуру на случай атаки, которая, тем не менее, может произойти в любой момент. Однако эти попытки показывают, что цели, при всей их ясности и обоснованности, труднее воплотить в жизнь, чем можно было ожидать. Опыт показывает, что в тот момент, когда они достигают определенного уровня конкретизации, их реализация отдаляется.

[33] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.

[34] CEB/2013/5, paras. 38–39.

128. **Обучение и повышение информированности как неоднозначный кандидат на общесистемное объединение ресурсов.** Одним из примеров многообещающего предложения, которое при более внимательном рассмотрении оказалось несколько неоднозначным, была область обучения и повышения информированности по теме кибербезопасности. Вопрос о сотрудничестве по программам обучения в системе Организации Объединенных Наций был рассмотрен в недавнем докладе ОИГ[35]. Один из выводов заключался в значительном дублировании усилий при создании аналогичных программ разными организациями. На первый взгляд ресурсы для обучения и повышения информированности по вопросам кибербезопасности кажутся естественным кандидатом для общесистемного взаимодействия и объединения ресурсов. Исходя из предположения, что бóльшая часть обучения конечных пользователей может быть стандартизирована, поскольку значительная часть соответствующих учебных материалов не обязательно должна относиться к конкретной организации из-за общего ландшафта угроз, один из первых совместных проектов, выполненных Специальной группой по информационной безопасности, включал разработку основных компонентов общей учебной программы по кибербезопасности для адаптации и использования ее членами. Подход, предусматривающий разработку учебной программы, по-видимому, получил определенную поддержку у ряда организаций, которые решили принять интерактивный учебный модуль по повышению информированности по вопросам информационной безопасности Секретариата Организации Объединенных Наций или привлекли Международный вычислительный центр Организации Объединенных Наций и его услугу повышения информированности по вопросам безопасности для адаптации и приспособления таких учебных материалов. Однако инспекторы не обнаружили прочного консенсуса среди участвующих организаций в отношении преимуществ общего подхода к обучению. Наоборот, несколько организаций решительно выступили против стандартизированного подхода, в частности сославшись на особенности, связанные с мандатом, или ограничения, налагаемые часто длительным процессом коллективной разработки, из-за которых совместно разработанные учебные материалы устаревают и их трудно заменить, а также неизбежно сходились к «наименьшему общему знаменателю», который может не соответствовать ожиданиям и требованиям пользователей без значительных последующих вложений, необходимых для дальнейшей адаптации и дополнения. В свете этих соображений ряд организаций разработали свои собственные учебные модули, иногда в сотрудничестве с внешними поставщиками, при этом затраты на них были достаточно заметными. **Инспекторы по-прежнему убеждены в том, что организациям системы Организации Объединенных Наций будет полезна некоторая согласованная подготовка, даже если ее, возможно, придется адаптировать для некоторых организаций.**

129. **Оптимизация ресурсов кибербезопасности.** Все опрошенные эксперты и руководители пришли к тому единому мнению, что подразделения Организации Объединенных Наций по отдельности и в совокупности являются небольшими акторами по сравнению со структурами частного сектора и что имеющиеся в их распоряжении ресурсы для противостояния более изощренным атакам извне со стороны организованной преступности или других финансируемых третьими сторонами атак и реагирования на них в лучшем случае ограничены. В то же время участвующие организации часто выделяют ресурсы на кибербезопасность изолированно и для своих собственных целей, иногда вынужденно в ответ на конкретное событие. Внутри системы имеется сильное ощущение того, что можно добиться повышения эффективности благодаря совместному подходу к кибербезопасности. Однако ответы организаций — участниц ОИГ о том, в каких областях объединение ресурсов достижимо и полезно, вызвали разноречивые отклики. Одной из областей, которая получила поддержку в качестве источника потенциальной экономии затрат, была более тесная координация взаимодействия с внешними поставщиками услуг, особенно с коммерческими структурами частного сектора. Многие организации подтвердили использование таких поставщиков, часто называя

[35] JIU/REP/2020/2.

одни и те же компании, предоставляющие те же или аналогичные услуги, в том числе по оценке рисков или уязвимостей, аудиту ИСО 27001 или конкретным программным решениям, позволяя считать, что каждая из них применяла в случае этих компаний свои процедуры проверки и контроля поставщиков, и при этом также самостоятельно оплачивала их услуги. Лишь несколько организаций указали, что они заключили между собой меморандумы о взаимопонимании или аналогичные договоренности, чтобы использовать процессы закупок друг друга или контракты на услуги, связанные с защитой кибербезопасности и реагированием, несмотря на действие соглашения о взаимном признании, подписанном 20 организациями. Инспекторы признают, что имеются факторы, ограничивающие широкомасштабную реализацию таких совместных инициатив, но, тем не менее, эти инициативы заслуживают большего внимания для повышения эффективности. С помощью собеседований и анкетирования инспекторы выявили ряд проблем, связанных с общими закупками и совместной закупочной деятельностью в целом. Различия между процедурами и правилами закупок в системе создают препятствия и ограничивают применение совместных закупок. Однако некоторые препятствия связаны не столько непосредственно с правилами и процедурами, сколько с рабочей культурой организаций, которая может не допускать открытого сотрудничества, вместо этого способствуя строгому организационному контролю. В этой связи некоторые препятствия включают различия в подходе между жестко централизованными и децентрализованными закупками, различия в порядке расчетов (например, авансовые платежи) и несогласованность систем ИКТ и систем расчетов с поставщиками, которые были названы в докладе ОИГ по вопросам закупок[36]. По крайней мере, если совместные закупки определенных услуг окажутся невозможными, участвующим организациям следует сделать все, что в их силах, чтобы максимально координировать свои усилия. В противном случае из-за несоответствий в практике закупок они рискуют создать стимул у коммерческих поставщиков взимать разную плату за одни и те же услуги в рамках системы, создавая форму конкуренции, которая приносит пользу только этим поставщикам, но наносит ущерб финансовым интересам заинтересованных организаций.

130. **Отсутствие действительно согласованных усилий на общесистемном уровне, кроме координации и частичных рабочих решений.** Можно сказать, что значительная известность и импульс, который кибербезопасность приобрела на самых высоких уровнях, создали оптимальные условия для решительного рывка в направлении создания общесистемного потенциала. Однако, несмотря на наличие в системе нескольких важных ресурсов, механизмов и инициатив, включая очевидную политическую волю, свидетельства прогресса в реализации этих вдохновляющих заявлений далеко не очевидны. На данный момент нет единой структуры, которой было бы официально поручено продвигать повестку дня согласованного подхода к кибербезопасности, а также разрабатывать и внедрять общие решения для организаций системы Организации Объединенных Наций. В настоящее время общесистемные усилия по кибербезопасности институционально сосредоточены вокруг механизмов межучрежденческой координации КСР, и они в определенной степени поддерживаются на рабочем уровне Международным вычислительным центром Организации Объединенных Наций в качестве поставщика определенных общих услуг для нескольких организаций системы Организации Объединенных Наций. В настоящей главе инспекторы изучают соответствующие институциональные и рабочие механизмы, включая, как представляется, определенную степень разногласий между ними и преобладающую межучрежденческую динамику в этом вопросе (приложение VI). Инспекторы также стремятся определить достигнутый к настоящему времени прогресс, преимущества и ограничения, присущие нынешней структуре, а также области, в которых могут иметься возможности более решительных коллективных действий при разработке ответных мер со стороны системы Организации Объединенных Наций в целом, насколько это практично и разумно.

[36] См. JIU/REP/2013/1.

B. Межведомственные механизмы, занимающиеся кибербезопасностью

131. **Долгая история внимания со стороны межведомственных механизмов.** Кибербезопасность под названием «информационная (системная) безопасность» фигурирует в дискурсе информационных технологий на общесистемном уровне со времен Административного комитета по координации. Еще в 1994 году целевой группе, созданной предшественницей Сети информационно-коммуникационных технологий (известной с 2018 года как Сеть по цифровизации и технологиям), было поручено проанализировать «руководящие принципы безопасности информационных систем организаций системы Организации Объединенных Наций», опубликованные в 1992 году[37], из чего можно заключить, что этот вопрос привлек к себе большое внимание и усилия еще раньше. Следует отметить, что руководящие принципы представляют собой всеобъемлющую и неожиданно прогрессивную попытку обобщить и предоставить рекомендации по различным аспектам кибербезопасности как на управленческом, так и на рабочем уровне, и несколько устаревшая терминология, используемая в документе, не должна отвлекать внимание от того, что значительная часть его содержания и рекомендаций остаются актуальными даже 30 лет спустя.

132. **Устойчивый интерес к скоординированному подходу к кибербезопасности.** Идея скоординированного реагирования на киберугрозы все еще фигурировала в официальных докладах 10 лет спустя, в 2002 году, когда члены КСР признали, что, «хотя задачи организаций в области безопасности делятся на разные категории (некоторые из них имеют банки чрезвычайно конфиденциальных и чувствительных данных), имеются важные проблемы, общие для всех организаций, которые необходимо решать в самом срочном порядке»[38]. В 2010 году термин «информационная безопасность», по-видимому, был заменен термином «кибербезопасность», которая приобрела значительный импульс, когда снова была поставлена задача выработки «плана общесистемного подхода» к кибербезопасности, описывающего последствия киберугроз для «всех секторов» как «возможного киберцунами»[39]. В последующие годы аналогичные заявления были сделаны на уровне Комитета высокого уровня по вопросам управления в отношении выявления «множества точек соприкосновения в отношении того, как наилучшим образом защитить [организации системы Организации Объединенных Наций] от сбоев в работе и угроз безопасности»[40], в то время как Сеть информационно-коммуникационных технологий заявила, что «повышение способности учреждений противостоять киберугрозам должно оставаться приоритетом»[41].

133. **Знаковые общесистемные документы по кибербезопасности и киберпреступности, принятые в 2013 и 2014 годах.** В 2010 году КСР поручил Комитету высокого уровня по вопросам управления и Комитету высокого уровня по программам совместно рассмотреть этот вопрос под руководством МСЭ и Управления по наркотикам и преступности (УНП) Организации Объединенных Наций , к которым позднее присоединились Конференция Организации Объединенных Наций по торговле и развитию (ЮНКТАД), ПРООН и ЮНЕСКО. Кульминацией этой сквозной инициативы стало утверждение в 2013 году концепции Организации Объединенных Наций по кибербезопасности и киберпреступности[42] и основанного на ней плана внутренней координации системы Организации Объединенных Наций по кибербезопасности и киберпреступности в 2014 году[43]. Хотя в обоих документах

[37] Advisory Committee for the Co-ordination of Information Systems, “Information System Security Guidelines for the United Nations Organizations”, New York, 1992.

[38] CEB/2002/HLCM/10, para. 8.

[39] CEB/2010/1, para. 53.

[40] CEB/2013/5, para. 36.

[41] CEB/2013/2, para. 58.

[42] Ibid., para. 85 and annex III (United Nations-wide framework on cybersecurity and cybercrime).

[43] United Nations system internal coordination plan on cybersecurity and cybercrime, November 2014, internal document.

основное внимание уделяется «внешнему» измерению работы Организации Объединенных Наций (т. е. программной деятельности, призванной поддержать государства-члены в их усилиях по этому вопросу), они обеспечивают прочную отправную точку определения «внутреннего» аспекта кибербезопасности системы (вставка 9). Тем не менее инспекторы отметили, что ни одна участвующая организация не упоминала концепцию или план во время подготовки обзора. Хотя план как таковой, по-видимому, не стал надежным ориентиром для системы, инспекторов заверили, что содержащиеся в нем основные принципы и элементы продолжают лежать в основе плана работы соответствующих межучрежденческих органов, действующих в этой сфере.

Вставка 9
Общесистемные рамки и план внутренней координации по кибербезопасности и киберпреступности

Утвержденная КСР на его второй очередной сессии 2013 года концепция системы Организации Объединенных Наций по кибербезопасности и киберпреступности закладывает основу для координации между организациями системы Организации Объединенных Наций в ответ на озабоченность государств-членов по поводу киберпреступности и кибербезопасности.

Концепция:

- вводит некоторые общие определения основных понятий и обрисовывает содержание темы;
- высвечивает пересечение соответствующих мандатов затрагиваемых структур;
- устанавливает основные принципы разработки программ и технической помощи, связанных с киберпреступностью и кибербезопасностью;
- содержит рекомендации по расширению сотрудничества при предоставлении технической помощи государствам-членам в этом отношении.

На основе этой концепции в 2014 году был разработан план внутренней координации системы Организации Объединенных Наций по кибербезопасности и киберпреступности для руководства внутренней координацией между организациями системы Организации Объединенных Наций в области кибербезопасности и киберпреступности, в котором Генеральный секретарь выделил пять тем для возможных совместных действий в рамках системы. По каждой теме в плане был изложен ряд общих принципов и направлений действий, которые организациям было предложено принять. В частности, исполнительным главам было рекомендовано разработать и принять к использованию обязательный компьютерный учебный курс по кибербезопасности для сотрудников на основе учебной программы, согласованной Сетью информационно-коммуникационных технологий, и создать межорганизационную группу реагирования на компьютерные инциденты. Это также были направления действий, которые, по мнению его Председателя, имеют отношение к работе Комитета высокого уровня по вопросам управления (CEB/2014/5, п. 72).

Особое значение для настоящего обзора имеет следующая тема:

Тема 1: Обеспечение действенной внутренней подготовки к противодействию киберугрозам в отдельных учреждениях и в рамках всей системы Организации Объединенных Наций, включая политические и ресурсные препятствия, которые могут помешать учреждениям действовать вместе для лучшей совместной защиты системы Организации Объединенных Наций, например, путем отражения кибербезопасности в системах оценки рисков и управления рисками.

134. **Специальная группа по информационной безопасности как главный общесистемный форум экспертов по кибербезопасности.** В целом было установлено, что межучрежденческий механизм кибербезопасности в системе Организации Объединенных Наций создан давно и в целом работоспособен. Специальная группа по информационной безопасности, созданная в 2011 году в качестве основного механизма в системе Организации Объединенных Наций для содействия межучрежденческому сотрудничеству и взаимодействию с целью оптимизации информационной безопасности в своих организациях-членах, подчиняется и получает указания от Сети по цифровизации и технологиям и действует под общим руководством Комитета высокого уровня по вопросам управления. В соответствии с ее кругом ведения, его членство прямо ограничено главными сотрудниками по информационной безопасности организаций — членов КСР или сотрудником в аналогичной должности. В случаях, когда такой должности не имеется, обычно соответствующую организацию представляет сотрудник по ИКТ. Методы работы Специальной группы по информационной безопасности включают ежегодный симпозиум с участием выступающих со стороны, исполнительную сессию для принятия официальных решений, проводимую во время ежегодного симпозиума, и создаваемые на конкретный срок рабочие группы, в которых ведущие организации добровольно ведут обсуждение по темам, представляющим интерес. Несколько организаций, не являющихся членами КСР, участвуют в работе Специальной группы по информационной безопасности в качестве наблюдателей без права голоса, в том числе Международный вычислительный центр Организации Объединенных Наций. Группу возглавляет на основе ротации один из ее официальных членов; на момент составления настоящего доклада эту роль взяло на себя Управление информационно-коммуникационных технологий Секретариата Организации Объединенных Наций.

135. **Подтверждение полезности основного межведомственного органа как форума для обмена мнениями.** Специальная группа по информационной безопасности приобрела значительный профессиональный авторитет в качестве официального форума, на котором специалисты Организации Объединенных Наций в области кибербезопасности регулярно собираются, чтобы обсудить проблемы, возможности и передовой опыт системы в целом. Анализ содержания недавних докладов симпозиумов Специальной группы по информационной безопасности подтверждает, что в Группе ведутся плодотворные дискуссии и уделяется внимание широкому кругу практических и стратегических вопросов, таких как облачная безопасность и управление облачными рисками, управление цифровой идентификацией, сравнительный анализ зрелости кибербезопасности, обучение по программе повышения осведомленности в области информационной безопасности и, в последнее время, идея общего центра обеспечения безопасности, а также консолидация служб аналитики угроз. В этой связи в своих ответах на анкету ОИГ около двух третей участвующих организаций отметили, что они считают Группу эффективным средством развития сотрудничества и взаимодействия между структурами Организации Объединенных Наций и высоко ценят существенный вклад ее членов, а также возможности обмена с внешними экспертами, в том числе экспертами из частного сектора. Многие члены высоко оценили усилия Председателя по содействию профессиональным обсуждениям и продвижению вперед по плану работы Группы. Некоторые недоработки, связанные с деятельностью Группы, уже устраняются, например редкое проведение симпозиумов Специальной группы по информационной безопасности и ограниченное взаимодействие между сессиями, которое, по мнению некоторых членов, необходимо активизировать, чтобы способствовать более непрерывному и неформальному диалогу. В свете очевидной необходимости этого был создан специальный канал обмена сообщениями для прямого неформального обмена между членами Специальной группы по информационной безопасности для оперативной связи и обмена информацией по мере необходимости. Усилия по поддержке повседневных обменов были положительно отмечены главными сотрудниками по информационной безопасности, которые также подтвердили, что они активно используют такие каналы в своей текущей работе.

136. **Межучрежденческий механизм обеспечения кибербезопасности на всех уровнях.** От самой Специальной группы по информационной безопасности до Сети

по цифровизации и технологиям и Комитета высокого уровня по вопросам управления была получена информация о том, что кибербезопасность активно обсуждается и признается критически важной. На уровне Сети по цифровизации и технологиям, которая объединяет руководителей подразделений ИКТ и получает доклады и рекомендации Специальной группы по информационной безопасности для утверждения и передачи Комитету высокого уровня по вопросам управления, «информационная безопасность и кибербезопасность» входит в число 10 целей Сети, поставленных в ее пересмотренном круге ведения 2019 года[44]. Можно сказать, что на практике Цифровая и технологическая сеть в целом высоко оценивает работу Специальной группы по информационной безопасности, поскольку только в нескольких случаях Сеть по цифровизации и технологиям отходила от позиции, занятой Специальной группой по информационной безопасности и большинство рекомендаций Группы были одобрены, иногда с изменениями. На уровне Комитета высокого уровня по вопросам управления, сыгравшего важную роль в разработке концепции 2013 года и плана координации 2014 года, кибербезопасность фигурирует в стратегических планах Комитета, включая его последний план (на 2017–2020 годы), как элемент стратегического приоритета управления рисками и повышения устойчивости. В последнем указано, что Комитет высокого уровня по вопросам управления будет прилагать новые усилия по содействию отслеживанию киберугроз и реагированию на них, включая реализацию мер по уменьшению последствий, на общесистемном уровне[45]. Однако доклады Комитета высокого уровня по вопросам управления, хотя и прямо признают, что кибербезопасность является проблемой, вызывающей озабоченность в общем плане, показывают, что конкретные рекомендации и вопросы, связанные с этой темой, редко доходят до Комитета. В этой связи инспекторы отмечают, что в своих ответах на анкету ОИГ только треть участвующих организаций сообщили, что они считают Специальную группу по информационной безопасности действенным средством создания импульса для действий на верхних уровнях механизма КСР.

137. **Выполнение рекомендаций и указаний Специальной группы по информационной безопасности зависит от ее членов.** В ходе настоящего обзора инспекторы установили, что межучрежденческая координация и сотрудничество в области кибербезопасности в системе Организации Объединенных Наций еще не принесли ожидаемых результатов. Несмотря на то, что ежегодно в рамках Специальной группы по информационной безопасности проводится большой объем концептуальной работы и этот вопрос находится в центре внимания высшего руководства, прогресс в направлении общих решений, общих или согласованных подходов и совместных проектов материализуется медленно. Для контекста стоит напомнить, что последняя итерация круга ведения Группы, пересмотренного в 2018 году[46], отражает его стремление делиться знаниями, опытом и решениями и, в частности, включает реализацию совместных проектов. Кроме того, позже в том же году после реорганизации Сети информационно-коммуникационных технологий в Сеть по цифровизации и технологиям и пересмотра мандатов каждой из ее подгрупп вновь переименованная Сеть пошла еще дальше, решив, что, помимо развития межучрежденческого сотрудничества и обмена знаниями в области информационной безопасности Специальной группе по информационной безопасности необходимо активнее разрабатывать и предлагать общие решения и инновации[47]. Однако поставленная Сетью по цифровизации и технологиям перед своей подгруппой цель более практической разработки решений для системы, по-видимому, не соответствует в каких-либо масштабах реальному потенциалу независимо от внутренних ресурсов ее членов и индивидуального уровня вовлеченности в этом отношении. Специальная группа по информационной безопасности де-факто не располагает действенным механизмом содействия выполнению и совместной реализации разработанных решений или договоренностей, достигнутых в межучрежденческом контексте. Отмечая, что ответственность за выполнение его рекомендаций не входит в число

[44] CEB/2019/HLCM/DTN/03/R1, p. 2.
[45] CEB/2016/HLCM/15, p. 13.
[46] CEB/2018/HLCM/ICT/3/Rev.1.
[47] CEB/2018/HLCM/ICTN/18, p. 6.

основных обязанностей координационного органа, отсутствие официально санкционированного «рабочего подразделения» для системы в целом, действующего под руководством коллектива старших сотрудников по информационной безопасности и служащего общим интересам, по мнению инспекторов, является одним из ключевых факторов, препятствующих продвижению к общесистемному подходу к кибербезопасности. Вопрос о том, могут ли другие существующие механизмы или органы в разумной мере заполнить пробел в реализации, более подробно рассматривается в следующих разделах настоящего доклада.

138. **Расширение полномочий главных сотрудников по информационной безопасности по отдельности и как группы.** Было установлено, что члены Специальной группы по информационной безопасности выполняют разные должностные обязанности, от рабочего уровня до стратегического уровня, при этом некоторые главные сотрудники по информационной безопасности занимают самые младшие должности категории специалистов, в то время как другие занимают должности руководителей среднего и высшего звена или возглавляют целые департаменты. Помимо технических знаний и культуры откровенного обсуждения, которая, по мнению ее членов, характерна для дискуссий Специальной группы по информационной безопасности, неоднородность ее членского состава, как сообщается, влияет на динамику внутри Группы и оказывает прямое влияние на возможности Группы по выработке авторитетных рекомендаций для системы. Поскольку в рамках структуры своей соответствующей организации каждый член Группы имеет разные полномочия — и связанные с ними ограничения — по принятию обязательств от имени своей организации в межучрежденческих отношениях, его возможности играть трансформирующую роль как внутри своей организации, так и вместе с другими на основе согласованных мер в масштабах всей системы ограничены. Специальная группа по информационной безопасности как координирующий орган сталкивается в этой связи с теми же проблемами, что и любой другой межучрежденческий механизм в отсутствие полномочий по принятию решений, влекущих за собой действия непосредственно на системном уровне, поэтому было бы нереалистично ожидать осуществления в рамках этого форума. В то же время она мало влияет на то, как результаты ее работы доводятся до высшего руководства каждой организации. Из материалов Сети по цифровизации и технологиям ясно следует, что эти ограничения хорошо понятны, о чем свидетельствует призыв Сети к своим членам — главам подразделений ИКТ — расширить возможности главных сотрудников по информационной безопасности, в числе прочего, путем делегирования им дополнительных полномочий[48]. Также стоит напомнить, что сама группа по информационной безопасности подчиняется Сети по цифровизации и технологиям, тем самым отражая преобладающую структуру и связанные с ней проблемы, наблюдаемые в большинстве организаций, где главный сотрудник по информационной безопасности подчиняется руководителю своего соответствующего подразделения ИКТ. Чтобы противодействовать ограничениям, обусловленным нынешней структурой, **инспекторы повторяют свой призыв к расширению внутренних должностных полномочий главного сотрудника по информационной безопасности, где такая должность учреждена, включая административные полномочия и независимость от ИКТ по мере возможности, а также к введению такой должности там, где ее не предусмотрено.** Что касается расширения полномочий главных сотрудников по информационной безопасности как группы, то инспекторы отметили, что, как правило, не было проявлено особого интереса к повышению места Специальной группы по информационной безопасности в межучрежденческом механизме путем выведения ее из подчинения Сети по цифровизации и технологиям и предоставления ей статуса сети, а результате чего Группа подчинялась бы непосредственно Комитету высокого уровня по вопросам управления. С одной стороны, аргументы против такой реорганизации включали общее распространение сетей, целевых групп и координационных форумов в рамках механизма КСР, что, как считается, само по себе вряд ли сможет способствовать продвижению в этом вопросе или реальному установлению его приоритета. С другой

[48] См., например, CEB/2017/HLCM/ICT/9, p. 8.

стороны, преобладала та точка зрения, что Специальная группа по информационной безопасности уже имеет в своем распоряжении адекватный и надежный канал, позволяющий выносить соображения кибербезопасности на передний план стратегических общесистемных дискуссий по линии Сети по цифровизации и технологиям и Комитета высокого уровня по вопросам управления. **Инспекторы подтвердили, что Специальная группа по вопросам информационной безопасности реально улучшила обмен информацией о кибербезопасности в системе Организации Объединенных Наций и должна и далее играть свою роль без изменения нынешней конфигурации архитектуры. Тем не менее инспекторы указывают на необходимость разработки механизма, обеспечивающего возможность осуществления Специальной группой по информационной безопасности — как самостоятельной структурой — стратегического руководства от имени КСР и системы Организации Объединенных Наций.**

C. Международный вычислительный центр Организации Объединенных Наций как поставщик услуг кибербезопасности

139. **Еще раз о нереализованном потенциале Международного вычислительного центра Организации Объединенных Наций.** В своем докладе об облачных вычислениях в 2019 году ОИГ уже призвала к дальнейшему изучению условий более эффективного использования нереализованного потенциала Международного вычислительного центра Организации Объединенных Наций. В тот момент кибербезопасность была выделена как одна из областей, где такой потенциал считался сформировавшимся и заслуживавшим дальнейшего изучения. Однако, имея в виду более широкую перспективу реформы рабочих процессов Организации Объединенных Наций, инспекторы видят возможность отдельного более целостного анализа Международного вычислительного центра Организации Объединенных Наций и его общего функционирования, бизнес-модели, структуры управления и мандата, возможно, даже за пределами отведенной ему роли поставщика услуг ИКТ для своих клиентов, которые в настоящее время включают, в частности, организации системы Организации Объединенных Наций. С момента его создания в 1971 году, которому предшествовал подробный доклад внешних ревизоров, который был заказан Генеральным секретарем в качестве председателя соответствующего межучрежденческого координационного механизма с мандатом на изучение средств электронной обработки данных и потребностей Организации Объединенных Наций, специализированных учреждений и МАГАТЭ и был представлен Генеральной Ассамблее[49], не проводилось такого анализа, который позволил бы проследить эволюцию Международного вычислительного центра Организации Объединенных Наций и критически изучить его возможности и унаследованный потенциал реагирования на более современные потребности системы. Отмечая предыдущие призывы ОИГ выявить возможные препятствия в этом отношении и без ущерба для выполнения официальных рекомендаций, содержащихся в настоящем докладе, **инспекторы полагают, что в будущем можно будет провести всеобъемлющий анализ Международного вычислительного центра Организации Объединенных Наций, особенно с целью определения структурных, финансовых и административных условий, которые позволили бы ему в полной мере реализовать свой потенциал стратегического партнера и ресурса системы Организации Объединенных Наций в целом.** Один из вопросов настоящего обзора, который определял изучение инспекторами, в частности, услуг в области кибербезопасности, предлагаемых Международным вычислительным центром Организации Объединенных Наций услуг, а также его структуры и видения им своего места в этой конкретной области, — имеются ли уже условия для того, чтобы он стал центром кибербезопасности системы Организации Объединенных Наций.

[49] A/8072.

Мандат и бизнес-модель

140. **Эволюция Международного вычислительного центра Организации Объединенных Наций с 1971 года по 2021 год.** В соответствии с резолюцией 2741 (XXV) Генеральной Ассамблеи Международный вычислительный центр Организации Объединенных Наций был учрежден меморандумом о договоренности, заключенным в 1971 году между Организацией Объединенных Наций, ПРООН и ВОЗ. Он был первоначально создан как межорганизационный центр предоставления «услуг электронной обработки данных» для трех его членов-основателей и других пользователей; с 1970-х годов его каталог услуг и клиентская база значительно изменились. Наиболее известный своими услугами хостинга и общей ИКТ-инфраструктурой, которую он предоставляет для поддержки систем общеорганизационного управления ресурсами многих своих клиентов, Международный вычислительный центр Организации Объединенных Наций расширил свою деятельность в таких разных областях, как облачные вычисления, роботизированная автоматизация процессов, блокчейн, разработка программного обеспечения, консалтинг в области ИКТ и кибербезопасность. Точно так же значительно выросла его клиентская база. С самого начала предполагалось, что его клиентская база может расшириться за счет новых клиентов: она выросла с первоначальных 3 до более чем 25 организаций системы Организации Объединенных Наций к 2003 году и примерно 70 клиентов в 2021 году, включая организации системы Организации Объединенных Наций и связанные организации, а также несколько не связанных с этой системой межправительственных организаций, международных НПО и международных финансовых институтов. В 2003 году в его учредительный документ были внесены поправки, устанавливающие более широкую правовую основу и более подробные правила участия в его работе; новый «мандат» конкретизирует и расширяет несколько основных положений, содержавшихся в первоначальном уставе. Он был отдельно принят всеми партнерскими организациями в рамках Руководящего комитета Международного вычислительного центра Организации Объединенных Наций и определяет структуру управления Центром, бизнес-модель и основные условия участия. Две основные функции Международного вычислительного центра Организации Объединенных Наций, отраженные в этом документе, заключаются в предоставлении услуг информационных технологий, включая эксплуатационное обслуживание и обучение, и в стремлении обеспечить, чтобы спектр его услуг соответствовал требованиям его организаций-партнеров.

141. **Основные принципы мандата и бизнес-модели Международного вычислительного центра Организации Объединенных Наций.** В обновленном круге ведения Международного вычислительного центра Организации Объединенных Наций подтверждена первоначальная цель его создания в качестве поставщика услуг для организаций системы Организации Объединенных Наций, а его предложение услуг тесно увязывается с конкретным спросом со стороны его клиентов. В то же время переформулирование его основных функций позволило ему быть максимально свободным в своем стремлении освоить новые направления работы, выходящие за рамки ограниченной области обработки данных, предоставив ему, в числе прочего, возможность предлагать услуги кибербезопасности даже без их прямого упоминания в его мандате. Одним из элементов, который был вновь подчеркнут и доработан в новом документе, стало понятие общей инфраструктуры и совместного обслуживания, цель которого заключается в достижении эффекта масштаба для клиентов Международного вычислительного центра Организации Объединенных Наций. Это называется моделью совместного обслуживания Международного вычислительного центра Организации Объединенных Наций, которая позволяет снизить стоимость его услуг прямо пропорционально увеличению числа клиентов, подписывающихся на соответствующую услугу. Наоборот, элементы, которые остались неизменными за 50 лет существования Международного вычислительного центра Организации Объединенных Наций, включают следующее: a) его модель возмещения затрат, которая фактически требует, чтобы все его продукты предварительно финансировались его клиентами на основе установленных потребностей и коллективного одобрения, что не предполагает получения им какой-либо прибыли или свободы действий в использовании бюджетных средств для исследований и

разработок; b) добровольный характер его каталога услуг, которыми организации могут по своему усмотрению воспользоваться на возмездной основе, принимая решение в отношении каждой конкретной услуги; и c) его зависимость от «принимающей организации» (ВОЗ), к которой Международный вычислительный центр Организации Объединенных Наций по-прежнему привязан административно и юридически, используя ее помещения и административное и юридическое сопровождение, чтобы иметь возможность заключать контракты, нанимать сотрудников, выделять средства и действовать в практическом плане.

142. **Сложная структура управления как отражение роли поставщика услуг, ориентирующегося на клиентов.** Чтобы поддерживать интерес клиентов к своему портфелю услуг, Центр разрабатывает их каталог в тесном сотрудничестве с представителями партнерских организаций в Руководящем комитете Международного вычислительного центра Организации Объединенных Наций. Этот орган, состоящий из 41 члена, не представляет всей клиентуры, обслуживаемой Центром, поскольку проводится различие между партнерскими организациями и пользователями его услуг, которые вместе называются его клиентами[50]. Только первые из них являются членами Руководящего комитета с правом голоса и могут определять направления развития деятельности Центра; клиенты, которые не являются также партнерскими организациями (т. е. просто «пользователи»), могут подписаться только на уже разработанные и предоставляемые услуги. Кроме того, при модели подписки на конкретные услуги не все члены Руководящего комитета являются клиентами услуг кибербезопасности, и наоборот (приложение VIII). Это теоретически связано с риском сдерживания развития или совершенствования таких услуг, которые могут быть необходимыми для некоторых, но не для всех организаций системы Организации Объединенных Наций. Что касается именно услуг кибербезопасности, то в 2020 году была создана неофициальная консультативная группа трех организаций, выделяющих основную часть финансирования услуг кибербезопасности (в настоящее время ПРООН, УВКБ и ФАО), с целью анализа предложения услуг с точки зрения качества и соответствия требованиям и определения дополнительных возможностей совместных решений. У группы есть прямой канал связи с Начальником службы кибербезопасности Международного вычислительного центра Организации Объединенных Наций, хотя последнее слово в разработке услуг остается за Руководящим комитетом. В целом архитектура управления Международным вычислительным центром Организации Объединенных Наций оказалась сложной, отражая многоуровневый характер его нынешней бизнес-модели. На вопрос о том, сможет ли эта архитектура в ее нынешнем виде воспринять и надлежащим образом обеспечить более заметную, даже обязательную роль системы, не требуя какой-либо значительной корректировки, не было очевидного ответа. Некоторые проблемы в этой связи более подробно рассматриваются в разделе D настоящей главы.

143. **Преимущества и недостатки бизнес-модели Международного вычислительного центра Организации Объединенных Наций.** После того, как данная услуга была разработана, все клиенты, подписавшиеся на нее, платят плату за использование, которая определяется и ежегодно пересматривается Руководящим комитетом и обычно корректируется в сторону уменьшения благодаря экономии за счет масштаба по мере того, как все больше клиентов подписываются на услугу, что приводит к уменьшению стоимости данной услуги для всех. В этом отношении модель строгого возмещения затрат, в соответствии с которой Международный вычислительный центр Организации Объединенных Наций действует с момента своего создания, имеет то преимущество, что обеспечивает высокую степень прозрачности в оценке стоимости услуг и постоянную координацию с клиентами, а

[50] Согласно поправке 2003 года к учредительному меморандуму о договоренности, термин «партнерская организация» означает любую организацию системы Организации Объединенных Наций, которая использует услуги Международного вычислительного центра и была принята Руководящим комитетом в качестве партнерской организации, в то время как термин «пользователи» означает те государства, межправительственные организации помимо партнерских организаций, НПО и другие государственные структуры, которые с разрешения Директора пользуются услугами Центра.

также контролирует объем предложения услуг, требуя максимально возможного согласования между тем, что действительно необходимо, и тем, что разрабатывается и производится в ответ на такую необходимость. Таким образом, мотив получения прибыли может быть практически исключен, и это один из аспектов, который отличает Международный вычислительный центр Организации Объединенных Наций от других поставщиков. В то же время не предусмотрено специального бюджета для поддержки основных руководящих и административных функций[51], и, таким образом, эти затраты должны быть включены в плату за оказываемые услуги. Оказалось, что его бизнес-модель, сочетающая в себе принципы возмещения затрат и совместного обслуживания, одновременно способствует и препятствует реализации стремления Центра к превращению в центр кибербезопасности для всей системы. Это создало ситуацию, в которой предложение услуг Международного вычислительного центра Организации Объединенных Наций зависит от клиентов, предоставляющих начальное финансирование для покрытия затрат на разработку новой услуги для удовлетворения спроса, в то время как многие могут позволить себе оплату разработанных таким образом услуг только после того, как на нее подпишется критическая масса клиентов. Этот аспект может систематически ставить в невыгодное положение менее мощные в финансовом отношении учреждения, чьи потребности в кибербезопасности могут отличаться от потребностей других организаций системы с большей бюджетной свободой, позволяющей им финансировать разработку конкретных новых услуг.

Каталог услуг кибербезопасности

144. **Международный вычислительный центр Организации Объединенных Наций как ключевой игрок в ландшафте кибербезопасности Организации Объединенных Наций.** За последние несколько лет Международный вычислительный центр Организации Объединенных Наций зарекомендовал себя в качестве ключевой заинтересованной стороны и ресурса кибербезопасности системы Организации Объединенных Наций. По свидетельству многих его клиентов, Центр накопил значительный опыт и возможности в области кибербезопасности и постепенно расширил свое предложение, включив в него 13 специализированных услуг в этой области, широко известных под торговой маркой Common Secure (диаграмма IX и приложение VII). Услуги охватывают как аспекты обеспечения кибербезопасности, так и рабочие аспекты, а также предлагаются Международным вычислительным центром Организации Объединенных Наций в качестве провайдера хостинга инфраструктуры, который также обеспечивает безопасность размещенных данных, систем и приложений; специализированного поставщика услуг кибербезопасности; консультанта по стратегическим и управленческим вопросам; или ликвидатора последствий инцидента, в зависимости от типа услуг, получаемых по подписке. Разнообразие предлагаемых Международным вычислительным центром Организации Объединенных Наций услуг кибербезопасности отражает тот факт, что спрос на эту линейку услуг среди ее клиентов значительно вырос. Несмотря на то, что продукты, связанные с кибербезопасностью, составляют лишь часть каталога услуг Центра и всего 6,1 % его общего объема финансирования (по состоянию на январь 2021 года), его (нынешняя и прошлая) клиентская база по таким продуктам включает 45 организаций, 21 из которых являются организациями — членами КСР (из в общей сложности 31) и 20 из которых являются организациями — участницами ОИГ (из в общей сложности 28). Несмотря на то, что около трети соответствующих организаций не охвачены услугами кибербезопасности Международного вычислительного центра Организации Объединенных Наций, включая, в особенности, Секретариат Организации Объединенных Наций, сегодня трудно представить себе кибербезопасность в системе Организации Объединенных Наций без учета роли и вклада Центра.

[51] The United Nations International Computing Centre Director’s report and financial statements for the biennium 2016–2017, published in April 2018, p. 46.

Диаграмма IX
Услуги кибербезопасности Международного вычислительного центра Организации Объединенных Наций (2021 год)

Услуги	*Число организаций — участниц Объединенной инспекционной группы (бывшие и нынешние клиенты)*
Общая аналитика угроз безопасности	17
Единый сервис электронной подписи	14
Реагирование на инциденты	11
Службы поддержки руководителей и главного сотрудника по информационной безопасности	11
Осведомленность об информационной безопасности	10
Защита от уязвимостей	7
Тестирование на проникновение	7
Услуги моделирования фишинга	6
Единая служба безопасности	5
Оценка безопасности облачной среды	5
Общая инфраструктура открытого ключа	3
Управление идентификацией и доступом	3
Общее безопасное управление информацией и проведение мероприятий	1

145. **Общая аналитика угроз безопасности как флагманская услуга кибербезопасности Международного вычислительного центра Организации Объединенных Наций.** Среди 13 услуг по кибербезопасности, предлагаемых Центром, некоторые уже привлекли значительное число клиентов в системе Организации Объединенных Наций и за ее пределами, в то время как другим еще предстоит обеспечить клиентскую базу. Одной из особо популярных услуг, на которую подписано 17 организаций-участников, что говорит о ее полезности, была услуга Центра «Общая аналитика угроз безопасности», которую можно считать флагманской службой кибербезопасности. Система Общая аналитика угроз безопасности получила самую положительную оценку подавляющего большинства клиентов Центра и удовлетворяет давние коллективные потребности, изложенные и неоднократно подтвержденные на системном уровне. Услуга объединяет различные внутренние и внешние, в том числе коммерческие и государственные, источники информации об угрозах, анализируемые и фильтруемые Международным вычислительным центром Организации Объединенных Наций для создания удобных информационных пакетов, адаптированных к условиям и аудитории Организации Объединенных Наций. На специальном совещании по кибербезопасности в октябре 2020 года Руководящий комитет Центра принял резолюцию, в которой всем партнерским организациям и клиентам предлагается делиться информацией об угрозах и инцидентах, связанных с безопасностью, в детализированном или анонимизированном виде с группой Общей аналитики для изучения и передачи другим организациям системы Организации Объединенных Наций. Инспекторы приветствуют это решение, но отмечают, что, согласно полученной информации, оно еще не реализовано повсеместно. В этой области большинство участвующих организаций, ответивших на анкету ОИГ, выразили интерес к более тесному сотрудничеству на общесистемном уровне, при этом некоторые из них отметили, что, помимо обмена информацией об угрозах и, в частности, признаках взлома, также было бы полезно обмениваться информацией о конкретных принятых мерах реагирования и устранения последствий. Однако последний аспект не получил единодушной поддержки среди экспертов, с которыми беседовали инспекторы, в основном по соображениям конфиденциальности. Тем не менее Общую аналитику угроз безопасности можно считать наиболее многообещающей услугой кибербезопасности с точки зрения ее естественного потенциала подписки на нее всех организаций

системы и реализации реальных преимуществ усиления защиты всей системы даже сверх того, что она уже достигла сегодня. При этом нет оснований считать, что такой же потенциал роста имеют все остальные услуги кибербезопасности в портфеле Международного вычислительного центра Организации Объединенных Наций.

146. **Разная оценка услуг кибербезопасности Международного вычислительного центра Организации Объединенных Наций.** Несмотря на строгий контроль клиентов Международного вычислительного центра Организации Объединенных Наций — в структурном плане — за предлагаемыми тем услугами, отзывы участвующих организаций относительно их удовлетворенности указанными услугами были достаточно разными: от «полного удовлетворения» до «полного неудовлетворения». Это может быть связано с несколькими факторами. С одной стороны, из 20 участвующих организаций, которые подписались или в прошлом подписались хотя бы на одну из услуг кибербезопасности Центра, есть некоторые различия в том, на сколько — и каких именно — услуг была подписана организация, которые, таким образом, были оценены как удовлетворительные или неудовлетворительные каждой из них. Различия в зрелости системы кибербезопасности соответствующей организации также могли повлиять на степень, в которой каждая из них могла в полной мере использовать во всех аспектах предлагаемую услугу и получать от нее положительные результаты. С другой стороны, некоторые из услуг, которые теперь выделены отдельно, раньше объединялись и предлагались в виде пакета, что само по себе вызывало некоторую критику из-за необходимости для организаций подписаться на части пакета, в которых они не нуждались, чтобы воспользоваться другими, необходимыми или желаемыми частями. Сообщается, что Международный вычислительный центр Организации Объединенных Наций прекратил эту практику в 2019 году и теперь предоставляет своим клиентам полную гибкость в выборе лучше всего подходящего им уровня и типа обслуживания. Кроме того, базовая оценка удовлетворенности может отражать более общую оценку взаимодействия или другого аспекта опыта работы с Центром, и как таковая менее надежна и недостаточно детализирована для того, чтобы считать ее окончательной. Ввиду этих ограничений и того, что в задачи инспекторов не входила оценка эффективности каждой услуги или каталога услуг Международного вычислительного центра Организации Объединенных Наций в целом, оказалось невозможно выявить очевидную закономерность в отношении типа, размера или степени развития тех организаций, которые высказали более критические или позитивные оценки Центра по сравнению с другими организациями. В целом можно сказать, что ряд организаций, больших и малых, высоко оценили Центр как поставщика услуг кибербезопасности, в то время как такое же число организаций заняли строго критическую позицию по отношению к Центру. Такая критика может в некоторых случаях отражать прошлые недостатки, которые могли быть преодолены благодаря последующим разработкам, и поэтому не должна заслонять настоящий и будущий потенциал Центра как поставщика услуг кибербезопасности. Однако высказанные оговорки вполне могут отражать нынешнее положение дел, сохранять свою силу или даже повторяться с течением времени, и поэтому к ним следует относиться со всей серьезностью. В любом случае регулярная и детальная оценка удовлетворенности клиентов может дать ценную информацию о том, где Центру было бы целесообразно приложить больше усилий с учетом замечаний своих клиентов и где он со временем мог бы привлечь дополнительных клиентов. Кроме того, всесторонняя оценка Международного вычислительного центра Организации Объединенных Наций как поставщика услуг кибербезопасности может быть полезной для получения более объективных гарантий общего качества и соответствия назначению услуг Центра в этой области.

147. **Названные преимущества взаимодействия с Международным вычислительным центром Организации Объединенных Наций.** Причины взаимодействия с Международным вычислительным центром Организации Объединенных Наций, как сообщили его клиенты, включали глубокое знание им системы и требований организаций системы Организации Объединенных Наций в силу его многолетнего опыта разработки индивидуальных услуг для них, того, что на него распространяются одни и те же административные правила и структуры, и его

взаимодействия с соответствующими межведомственными форумами. Кроме того, Центр выделил несколько сравнительных преимуществ, которые отличают его от поставщиков коммерческих услуг, в том числе следующих: последовательное снижение стоимости услуг по мере роста клиентской базы; отсутствие ориентации на прибыль и связанная с этим заинтересованность в сохранении доступных цен, в том числе для организаций с меньшим бюджетом, ищущих недорогие варианты; неотъемлемая и общая цель — сделать систему более безопасной для всех, в том числе для себя как члена системы; а также способность наблюдать, адаптироваться и учиться у своих клиентов из первых рук, масштабируя извлеченные уроки непосредственно на благо коллектива. Взгляд с высоты птичьего полета на систему в целом и на все ее части также отличает Международный вычислительный центр Организации Объединенных Наций от коммерческих поставщиков, которые, как правило, видят только части более крупной головоломки и, таким образом, гарантирует, что он способен принести повышенную отдачу за пределами индивидуального контекста любого конкретного клиента. Еще один аспект, который инспекторы сочли убедительным, заключался в том, что, несмотря на существующие межучрежденческие механизмы и дополнительный уровень представительного управления в виде Руководящего комитета Центра, нет единой структуры, которая была бы внутренне мотивирована преследовать явно коллективные интересы системы, а не индивидуальные или, в лучшем случае, совокупные — и часто несовместимые — интересы. Международный вычислительный центр Организации Объединенных Наций видит себя нейтральным, аполитичным и — благодаря своей модели возмещения затрат — бескорыстным брокером общесистемных решений в этой области, руководствующимся общим благом, а не какими-либо соображениями острой нехватки ресурсов, которые могут влиять на членов его Руководящего комитета и вовлекать их в потенциальный конфликт интересов.

148. **Названные недостатки Международного вычислительного центра Организации Объединенных Наций как поставщика услуг кибербезопасности.** Наоборот, несколько организаций дали менее похвальную оценку Международному вычислительному центру Организации Объединенных Наций как поставщику услуг кибербезопасности, конкретно критикуя те в аспекте эффективности затрат по сравнению с возможными предложениями коммерческих поставщиков. У некоторых сложилось впечатление, что сторонние компании владеют новейшими знаниями и средствами на уровне, превышающем возможности, которых Международный вычислительный центр Организации Объединенных Наций или любая организация могли бы достичь даже после значительных инвестиций. Таким впечатлениям противостояли другие голоса среди клиентов, которые сообщили о подлинном скачке в опыте и киберподготовленности Центра за последние годы, что подтверждается значительными инвестициями его руководства в сертификацию соблюдения стандартов ИСО, привлечением экспертов разного профиля и созданием круглосуточного единого центра обеспечения безопасности, расширяющего возможности круглосуточного контроля Международного вычислительного центра Организации Объединенных Наций и его каталог услуг. Однако при всех этих усилиях остается ощущение сохраняющегося пробела в уровне специальных познаний и эффективности затрат, который — возможно, по объективным причинам — Центру сложно преодолеть. Далее указывалось на то, что аналогичные услуги могут предоставляться по более конкурентоспособной цене частным сектором, и некоторые респонденты считали, что, несмотря на экономию за счет масштаба, связанную с моделью совместного обслуживания, Центр взимает слишком высокую плату за некоторые из своих услуг, причем непрозрачным образом, из-за чего они оказываются недоступными или малопонятными для одних и недостаточно компенсируются отдачей в других областях для других. Международный вычислительный центр Организации Объединенных Наций фактически признал, что конкуренция с частным сектором выходит за пределы его возможностей и даже в некоторых отношениях контрпродуктивна. Учитывая его бизнес-модель, стоимость его услуг, как правило, снижается при присоединении новых клиентов, в то время как стоимость во многих случаях, собственно, является входным барьером для организаций, желающих подписаться на услуги. Этот парадокс можно частично разрешить, например, путем вливания некоторого менее строго связанного финансирования в нужных

направлениях, чтобы Центр мог снизить некоторые из своих расценок, возможно, до более низкого уровня, чем у поставщиков частного сектора, без необходимости пытаться их полностью заменить. Отмечая, что нет смысла конкурировать с частным сектором в тех областях, где он позволяет получить более высокую отдачу затрат и более эффективен, исполнительным главам следует изучить вопрос о том, может ли Международный вычислительный центр Организации Объединенных Наций действовать в качестве связующего звена между коммерческими поставщиками и их клиентам в системе Организации Объединенных Наций, чтобы снизить сумму контракта и добиться экономии за счет масштаба и, в конечном итоге, усилить переговорные позиции. Кроме того, в сочетании с независимой оценкой его услуг кибербезопасности, предложенной выше, Международный вычислительный центр Организации Объединенных Наций мог бы провести критический анализ своего каталога услуг кибербезопасности, чтобы четче выделить те области обслуживания, где Центр может иметь сравнительные преимущества и рассмотреть возможность расширения своих усилий. В конечном итоге инспекторы отметили, что, несмотря на иногда резкую критику Международного вычислительного центра Организации Объединенных Наций как поставщика услуг кибербезопасности, система использует предлагаемые им услуги.

149. **Возможности улучшений в пределах нынешнего мандата Международного вычислительного центра Организации Объединенных Наций.** Хотя некоторые организации выступают за официальное укрепление статуса Международного вычислительного центра Организации Объединенных Наций как поставщика кибербезопасности для системы Организации Объединенных Наций, инспекторы считают, что многое может быть достигнуто в рамках нынешнего мандата Центра, пересмотренного в 2003 году, который уже обеспечивает прочную основу для реализации решений, которые могут быть внедрены при несколько более активном участии всех заинтересованных сторон. Даже если по соответствующим причинам потребуются изменения в его мандате, это входит в коллективную компетенцию его организаций-учредителей и тех организаций, которые подписали поправки к его учредительному документу в 2003 году, и не потребует решений со стороны Генеральной Ассамблеи до проведения более всестороннего анализа Международного вычислительного центра Организации Объединенных Наций как организации, его достижений на сегодняшний день и возможных структурных причин его нереализованного потенциала, которые могут быть устранены в результате такого решения. По мнению инспекторов, одним из важнейших аспектов, требующих решения без дальнейших проволочек или дополнительных предварительных условий, было бы выяснение причины и устранение широко распространенного разрыва между существующими структурами и механизмами и некоторыми ограничениями в нынешней схеме финансирования, как подробно указано ниже.

D. Улучшение связи между общесистемным стратегическим руководством и функциональным потенциалом

Устранение разрыва между Специальной группой по информационной безопасности и Международным вычислительным центром Организации Объединенных Наций

150. **Официальные ограничения связи между Специальной группой по информационной безопасности и Международным вычислительным центром Организации Объединенных Наций.** В свете значительного дублирования между организациями, представленными в механизмах межучрежденческой координации, с одной стороны, и Руководящим комитетом Международного вычислительного центра Организации Объединенных Наций — с другой (приложение VIII), можно было бы предположить, что Специальная группа по информационной безопасности — это орган, который обеспечивает стратегическое руководство и руководство по общим решениям в области кибербезопасности, которые могут быть подходящими для организаций системы Организации Объединенных Наций, в то время как Центр функционирует как подразделение системы, которой поручены вопросы

практического внедрения. Однако эти обе структуры не связаны формально и не действуют совместно на практике. Формально Специальная группа по информационной безопасности выполняет только роль по координации и обмену информацией и не уполномочена каким-либо образом давать указания Международному вычислительному центру Организации Объединенных Наций, в то время как последний выполняет решения своего Руководящего комитета в отношении услуг, которые будут разработаны для его партнеров и клиентов, в число которых входят не все организации системы Организации Объединенных Наций. На практике институциональный разрыв между обоими структурами может не быть решающим фактором, но он, вероятно, внес свой вклад в динамику, которая может дорого обойтись системе с точки зрения эффективности из-за упущенных возможностей более непосредственного сотрудничества.

151. **Ряд факторов, объясняющих напряженное взаимодействие на практике.** Следует отметить, что Международный вычислительный центр Организации Объединенных Наций получил статус наблюдателя в Специальной группе по информационной безопасности и участвует в обсуждениях последней без права голоса или вынесения вопросов на обсуждение. Однако Центр заявил, что ему фактически было отказано в возможности продвигать свой каталог услуг на форуме Специальной группы по информационной безопасности или запрашивать прямые отзывы о своих решениях в его рамках. Такую позицию можно частично объяснить характером Международного вычислительного центра Организации Объединенных Наций как межорганизационной структуры, а не организации, статус которой может предоставить ему возможность членства в КСР и, таким образом, полные права на участие. Также указывалось на то подспудное мнение, что Международный вычислительный центр Организации Объединенных Наций является прежде всего поставщиком, а не партнером организаций системы, что еще больше затрудняет его полную интеграцию в существующие межучрежденческие механизмы. Учитывая его организацию, ориентированную на клиентов, и его роль поставщика специализированных вычислительных услуг для своих партнеров — организаций, трудно отрицать, что отношение к нему как к поставщику имеет свои причины. В то же время Центр открыто представляет себя структурой Организации Объединенных Наций и полноправным членом системы Организации Объединенных Наций. Так, его руководство всячески заявляет о своей готовности превратить Международный вычислительный центр Организации Объединенных Наций в центр кибербезопасности системы Организации Объединенных Наций, если ему будет предоставлена такая возможность, в то время как некоторые организации даже высказали мнение, что Центр должен сделать кибербезопасность своим основным видом деятельности. Однако до тех пор, пока не будут рассмотрены и решены проблемы, касающиеся динамики между располагающими мандатами межучрежденческими механизмами системы и Международным вычислительным центром Организации Объединенных Наций как ведущим поставщиком услуг кибербезопасности, который мог бы взять на себя роль функционального звена системы в этой области, этот сценарий, вероятно, останется вне досягаемости.

152. **Де-факто параллельные структуры.** Одним из примеров, показывающих, как динамика между межучрежденческим механизмом и Международным вычислительным центром Организации Объединенных Наций привела к неожиданным решениям поставленных задач, но одновременно привела к дублированию в области кибербезопасности, — Конференция по общей безопасности, организуемая Центром. С 2019 года конференция служит для клиентов службы кибербезопасности Центра средством обмена информацией по вопросам, представляющим общий интерес, на оперативном уровне и предоставления отзывов о предоставляемых услугах. Это мероприятие стало регулярным и заметным в календаре кибербезопасности, получая много позитивных отзывов от его участников, многие из которых являются организациями системы Организации Объединенных Наций, которые также представлены в Специальной группе по информационной безопасности. В некотором смысле можно сказать, что Конференция по общей безопасности заполнила пробел для Международного вычислительного центра Организации Объединенных Наций, который стремился напрямую взаимодействовать

с организациями через Специальную группу по информационной безопасности, но не смог сделать это столь продуктивно и конкретно, как ему хотелось бы, в отношении своей цели по развитию партнерства с системой и практических аспектов предложения им своих услуг. Кто-то может даже сказать, что конференция стала де-факто ведущим форумом для значительной части системы как прямое следствие неспособности существующего координационного механизма Специальной группы по информационной безопасности начать в практической плоскости дискуссии, в большей степени нацеленной на выработку решений. Обратной стороной этих инициативных и новаторских разработок стало то, что конференция, возможно, перенаправила некоторые обсуждения, которые вполне могли проводиться в рамках Специальной группы по информационной безопасности, на другой форум, который теоретически в основном открыт для клиентов Международного вычислительного центра Организации Объединенных Наций, а не системы в целом. Существование этих двух — фактически параллельных, а не взаимодополняющих — структур, служащих очень похожим целям, одной под эгидой КСР, а другой — под эгидой Международного вычислительного центра Организации Объединенных Наций, чревато риском дальнейшего разобщения и конкуренции, что приведет к неэффективности, дублированию и параллелизму. Это один из негативных побочных эффектов, вызванных неудовлетворительной организацией динамики между ними.

153. **Необходимость наращивания синергизмов.** Эти замечания должны учитываться обеими структурами в попытках улучшить свое взаимодействие. С одной стороны, Специальной группе по информационной безопасности необходимо активизировать свои коллективные усилия по выполнению своего мандата в более стратегическом смысле, определяя области, в которых можно найти общие решения, если не для системы в целом, то хотя бы для кластеров организаций, где улучшение состояния кибербезопасности могло бы привести к ее усилению во всей системе. Если она не сделает этого, используя авторитетный голос представителя всей системы, есть вероятность, что Международный вычислительный центр Организации Объединенных Наций будет вынужден вмешаться и занять это пространство, которое таким образом будет по-прежнему ограничено кругом обслуживаемых им клиентов. В то же время использование Международным вычислительным центром Организации Объединенных Наций возможности вакуума, непреднамеренно созданного Специальной группой по информационной безопасности, в принципе, полезно для системы из-за его инновационного потенциала, но это не должно происходить в отрыве от официального органа, отвечающего за общесистемную координацию и сотрудничество в области кибербезопасности. Обе организации обязаны активно искать способы улучшить динамику между ними, с помощью будь то формальных или неформальных мер. В этой связи считается, что ряд услуг Центра в области кибербезопасности, популярные среди клиентов, были вдохновлены или непосредственно вызваны к жизни обменами, проводимыми в рамках Специальной группы по информационной безопасности, даже если последняя не заказывала их в любом формальном смысле. Если Международный вычислительный центр Организации Объединенных Наций по-прежнему намерен добиваться превращения в узел кибербезопасности всей системы, а не только своих клиентов, то тем более он не может позволить себе оставаться в стороне от экспертного сообщества, представляющего коллективные потребности организаций, которые обслуживались бы таким узлом. Кроме того, Специальная группа по информационной безопасности, как коллектив, отчасти держит в своих руках ключи к более конструктивному сотрудничеству в этой области. Возможности синергизмов и большей взаимодополняемости есть, но на сегодняшний день они реализованы не полностью.

154. **Рассмотрение участвующими организациями возможности использования услуг кибербезопасности Международного вычислительного центра Организации Объединенных Наций.** В качестве одного из способов устранения существующего разрыва между обеими структурами высказывались предложение о введении обязательного пользования услугами кибербезопасности Международного вычислительного центра Организации Объединенных Наций обязательным для организаций системы Организации Объединенных Наций. Утверждалось, что это также ускорит потенциальное повышение эффективности и сокращение затрат за счет

расширения масштабов и охвата Центра как поставщика совместно используемых услуг. Это видение разделяли не все и на самом деле может быть контрпродуктивным. С одной стороны, это лишило бы организации системы Организации Объединенных Наций возможности участвовать в оценке и принятии решений о предлагаемых услугах, наилучшим образом соответствующих их требованиям, путем навязывания и введения искусственной монополизации предложения услуг поставщиком извне. С другой стороны, внутри Международного вычислительного центра Организации Объединенных Наций существуют работоспособные механизмы управления, которые уже позволяют вести здоровое общение между его исполнительным руководством и его клиентами по вопросам формирования услуг кибербезопасности. Инспекторы считают, что вмешиваться в эти механизмы нецелесообразно и не нужно. **Однако уже в 2019 году инспекторы призвали организации системы Организации Объединенных Наций и Международный вычислительный центр Организации Объединенных Наций расширить точки соприкосновения для дополнения имеющегося потенциала организаций новыми видами совместного обслуживания**[52]**.** В частности, инспекторы считают, что некоторые из причин, которые в прошлом могли побудить отдельные организации отказаться от подписки на услуги кибербезопасности Центра или воздержаться от них, возможно, стоит проанализировать вновь. Решение на этот счет должно быть нюансированным, в идеале (пере)оценивающим каждую предлагаемую услугу кибербезопасности по ее достоинству. Некоторые из услуг действительно могут еще не достичь уровня зрелости или в достаточной степени отвечать потребностям организаций, чтобы все члены системы приняли решение подписаться на них. Международный вычислительный центр Организации Объединенных Наций должен продолжать свои усилия по устранению любых пробелов в этом отношении. Инспекторы также признают индивидуальность каждой организации. В конечном итоге ответственность за принятие соответствующих решений, основанных на их конкретных требованиях, лежит на организациях, особенно с учетом разнообразия информационных систем, приложений и других технических механизмов, созданных внутри организаций или отраженных в договорах с внешними поставщиками.

Добровольные донорские взносы в дополнение к финансированию общих решений для системы

155. **Добровольные взносы как средство прямой поддержки.** По мнению инспекторов, настало время рассмотреть вопрос об использовании добровольных взносов в качестве дополнительного механизма финансирования для привлечения дополнительных прямых ресурсов для защиты общей кибербезопасности системы. Возможность привлечения добровольных взносов, предназначенных для общесистемных мер, может убрать некоторые камни преткновения, препятствующие реализации общих решений в области кибербезопасности, поскольку нехватка ресурсов в участвующих организациях, вероятно, повлияла на их готовность вносить вклад в общий пул финансирования. Предоставление системе возможности использовать источник донорских взносов, не зависящий от отдельных бюджетов ее членов, может отчасти снизить нажим, вызванный, с одной стороны, крайне ограниченной свободой действий, заложенной в эти бюджеты со столь многими приоритетами задач, конкурирующих за все более дефицитные средства организаций, и, с другой стороны, моделью возмещения расходов Международного вычислительного центра Организации Объединенных Наций. В последнем случае это позволит развивать инновационные направления обслуживания своих партнеров — организаций, особенно тех, которые располагают менее развитым внутренним потенциалом или имеют меньше ресурсов для создания механизмов кибербезопасности в целом. В сочетании с его моделью общих услуг такой подход мог бы и дальше способствовать снижению затрат благодаря сохранению низкой платы за обслуживание и, вероятно, способствовал бы привлечению дополнительных клиентов, тем самым усиливая положительные эффекты. Будет ли наиболее целесообразно передать механизм привлечения и расходования таких добровольных взносов в

[52] JIU/REP/2019/5.

непосредственное ведение системы как единого целого, например в виде целевого фонда, которым должен будет распоряжаться секретариат КСР с учетом существенного вклада Специальной группы по информационной безопасности, или Международного вычислительного центра Организации Объединенных Наций в качестве де-факто признанного поставщика многих общих решений для системы — эти вопросы, в частности, инспекторы рассматривали в консультации с соответствующими собеседниками. Изучив различные варианты такого рода, инспекторы пришли к выводу, что лучше всего передать такой фонд в распоряжение структуры, которая будет требовать оперативного контроля над расходами на повседневной основе при разработке необходимых услуг, а именно Международного вычислительного центра Организации Объединенных Наций.

156. **Целевой фонд кибербезопасности.** В принципе мандат Международного вычислительного центра Организации Объединенных Наций с момента внесения в него поправок в 2003 году включает положения, позволяющие ему привлекать добровольные взносы, и в недавнем прошлом имелся прецедент, когда по этому каналу финансировался конкретный проект. На сегодняшний день этот механизм используется недостаточно, и его стратегическое использование для упреждающей разработки услуг, которые будут совместно использоваться всеми или несколькими организациями системы Организации Объединенных Наций, может привести к изменению положения дел. Более широкое распространение информации о существовании такой возможности и уточнение условий, при которых она может быть использована, может предоставить возможность государствам-членам, желающим вносить непосредственный вклад в повышение кибербезопасности во всей системе, в соответствии с условиями, применимыми к соответствующему целевому взносу, для поддержки совместных решений в области кибербезопасности. Это также способствовало бы выполнению рекомендации ОИГ 2019 года о механизме финансирования, позволяющем Международному вычислительному центру Организации Объединенных Наций проводить исследования и разработки вне рамок его модели возмещения затрат, что могло бы принести дополнительную пользу его клиентам из числа организаций системы Организации Объединенных Наций. Поэтому инспекторы рекомендуют, чтобы после соответствующих консультаций директор Международного вычислительного центра Организации Объединенных Наций учредил целевой фонд кибербезопасности специально для проектирования и разработки общих услуг кибербезопасности, которые больше всего необходимы системе. Чтобы дополнительно отделить этот механизм от других источников финансирования, предоставляемых в распоряжение Центра его партнерами-организациями и клиентами, было бы целесообразно создать специальный целевой фонд, предусмотрев для него особые условия, гарантирующие, что его управление не будет воспроизводить существующих структурных перекосов, потенциальных конфликтов интересов или неконструктивной динамики, обусловленной перекрывающимся и тем не менее различным составом членов его Руководящего комитета и соответствующих общесистемных органов.

157. **Практические вопросы создания целевого фонда.** Соответственно, круг ведения такого механизма финансирования будет ключом к его успеху. Он должен прояснить роль и обязанности различных заинтересованных сторон, виды услуг, которые предполагается финансировать, и процедуры прозрачного распределения средств, включая соответствующие требования к отчетности. В частности, фонд должен быть создан для использования в основном для целей, приносящих организациям системы осязаемые результаты. Главная цель фонда может заключаться в финансировании исследований и разработок с целью предоставления услуг кибербезопасности, вызывающих явный интерес организаций, но не обеспеченных критической массой пользователей, готовых выделить часть необходимого начального финансирования. Точно так же фонд можно было бы использовать для увеличения объема или глубины уже предоставляемых услуг, на которые есть явный спрос и которые требуют начального финансирования, или стоимость которых необходимо будет снизить, чтобы дополнительное число организаций могли быстрее подписаться на них. Хотя целевой фонд, как правило, подчиняется финансовым правилам и положениям ВОЗ, в соответствии с которыми работает Международный

вычислительный центр Организации Объединенных Наций, имеется возможность встроить в его управление элемент консультаций с компетентными межучрежденческими органами. Это поможет получить совместные решения, которые будут разрабатываться для системы в целом, а не только для клиентов Центра, и тем самым еще больше улучшит использование имеющихся ресурсов. Учитывая ее роль в обеспечении основы для создания Международного вычислительного центра Организации Объединенных Наций, Генеральной Ассамблее предлагается принять к сведению рекомендацию о создании целевого фонда кибербезопасности и предложить государствам-членам внести в него взносы.

158. Ожидается, что выполнение следующих ниже рекомендаций улучшит координацию и сотрудничество между организациями системы Организации Объединенных Наций.

Рекомендация 3

Директору Международного вычислительного центра Организации Объединенных Наций следует стремиться к созданию не позднее конца 2022 года целевого фонда донорских взносов, который дополнил бы возможности Центра по проектированию, разработке и предложению общих услуг и решений для улучшения состояния кибербезопасности в организациях системы Организации Объединенных Наций.

Рекомендация 4

Генеральной Ассамблее Организации Объединенных Наций следует не позднее чем на своей семьдесят седьмой сессии принять к сведению рекомендацию, адресованную директору Международного вычислительного центра Организации Объединенных Наций, о создании целевого фонда для совместных решений по кибербезопасности и предложить государствам-членам, желающим улучшить состояние кибербезопасности в организациях системы Организации Объединенных Наций, сделать взносы в целевой фонд.

E. Возможности более тесного согласования физической безопасности и кибербезопасности

159. **Кибербезопасность не охватывается системой обеспечения безопасности Организации Объединенных Наций.** В своей резолюции 59/276 Генеральная Ассамблея учредила Департамент охраны и безопасности, наделенный общесистемным мандатом определять правила и систему подотчетности, а также рабочие стандарты и процедуры для обеспечения безопасности персонала и имущества Организации Объединенных Наций. Возможно, неудивительно, что мандат, возложенный на Департамент охраны и безопасности еще в 2004 году, до существенных общесистемных изменений в области кибербезопасности в 2013 и 2014 годах, не содержит ни прямого упоминания кибербезопасности, ни упоминания о защите данных и цифровых ресурсов или киберсреды в более широком смысле[53]. Несмотря на то, что Департамент по вопросам охраны и безопасности указал, что рекомендации по информационной безопасности действуют в масштабах всей системы, система обеспечения безопасности и соответствующие установочные документы Организации Объединенных Наций еще должны определить точки соприкосновения между физической безопасностью и кибербезопасностью с целью

[53] Департамент охраны и безопасности указал, что конкретными категориями рисков для безопасности, охватываемых Департаментом и системой обеспечения безопасности Организации Объединенных Наций, являются массовые беспорядки, вооруженный конфликт, терроризм, преступления и угрозы (непреднамеренные).

определения ответственности различных заинтересованных сторон системы в этом плане. Инспекторы приветствуют то, что в Руководстве по политике безопасности системы обеспечения безопасности Организации Объединенных Наций был предусмотрен раздел «Информационная безопасность — конфиденциальность, классификация и реакция», и они считают это признаком определенного признания важности соображений кибербезопасности для функции физической охраны и безопасности. Однако соответствующая глава еще не подготовлена, и Департамент охраны и безопасности выразил оговорки относительно необходимости такой отдельной главы на данный момент. Между тем, как подтвердило Управление по правовым вопросам и вопреки тому устоявшемуся толкованию, что упоминания защиты собственности и имущества в соответствующих конвенциях и соглашениях с принимающей страной понимаются как охватывающие цифровые ресурсы и коммуникации, можно считать, что ни мандат, ни соответствующая нормативно-правовая база, регламентирующая функции физической охраны и безопасности в системе Организации Объединенных Наций, сегодня не охватывают кибербезопасности.

160. **Межучрежденческая сеть обеспечения безопасности и Специальная группа по информационной безопасности.** Круг ведения Межучрежденческой сети обеспечения безопасности, которая оказывает содействие Комитету высокого уровня по вопросам управления в его всеобъемлющем обзоре стратегий и связанных с ресурсами вопросов, касающихся системы обеспечения безопасности Организации Объединенных Наций, и контролирует реализацию правил, практики и процедур обеспечения безопасности всеми участниками системы Организации Объединенных Наций, также не содержит конкретного упоминания кибербезопасности. Исследование, проведенное ОИГ, подтверждает, что Межучрежденческая сеть обеспечения безопасности затрагивала эту тему только в редких случаях и в основном с точки зрения использования ИКТ для совершенствования общих процессов физической безопасности, например для управления идентификацией и доступом (например, изучение вариантов биометрических идентификационных карт доступа для входа в физические помещения, а также в цифровое пространство) или процедур сертификации с помощью ИКТ применительно к разрешениям на поездку, предоставляемым службой безопасности. Недавно, в 2019 году Сеть по цифровизации и технологиям приняла рекомендацию Специальной группы по информационной безопасности о налаживании координации между Группой и Межучрежденческой сетью обеспечения безопасности «по вопросам, представляющим взаимный интерес»[54]. Однако инспекторы не смогли найти подтверждений того, что заявленное намерение материализовалось вне связи с конкретными проектами. Соответствующим межучрежденческим механизмам предлагается продолжить изучение практических способов установления более регулярного канала связи для расширения сотрудничества. В этой связи инспекторам было высказано мнение, что взаимное участие председателей Сети и Группы в совещаниях обеих структур могло бы способствовать обмену полученными уроками.

161. **План взаимодействия с национальными властями в отношении киберинцидентов.** Одна из областей, в которой процедуры, установленные для обеспечения физической охраны и безопасности, могут послужить источником вдохновения для киберсреды, связана с взаимодействием с национальными властями в отношении кибератак. В главе II (пп. 35–37) настоящего обзора инспекторы достаточно подробно осветили сложный внутренний процесс, ведущий к принятию решения о том, обращаться ли к национальным властям, оставив в стороне вопрос о том, что произойдет, когда такое решение будет принято, и как будет развиваться общение с соответствующим государственным органом. Это далеко не так просто, поскольку наиболее подходящие органы такого рода могут быть разными в зависимости от профильного министерства, в котором созданы национальные группы реагирования (или готовности) на компьютерные чрезвычайные ситуации, или группы реагирования на инциденты в области компьютерной безопасности (например, министерства внутренних дел, обороны, связи или технологий, в зависимости от

[54] CEB/2019/HLCM/DTN/02, CEB/2019/HLCM/DTN/07, pp. 4–5.

страны), и в том же государстве могут существовать параллельные структуры в рамках национальной разведслужбы с полномочиями бороться с кибератаками с возможными политическими последствиями. Поэтому на уровне государства может и не быть центрального координационного центра, которому было бы официально поручено получать соответствующие сообщения от организаций системы Организации Объединенных Наций, и это может затруднить надлежащую передачу информации. Применительно к кризисам, связанным с физической безопасностью, Руководство по политике безопасности Системы обеспечения безопасности Организации Объединенных Наций предусматривает, что назначенные должностные лица «просят правительство принимающей страны назначить контактных лиц с полномочиями мобилизовать и координировать поддержку, когда кризис затрагивает Организацию Объединенных Наций в стране»[55]. Аналогичный подход можно было бы изучить в качестве схемы для киберинцидентов, признав в то же время, что назначенным должностным лицам были бы полезны экспертные рекомендации службы кибербезопасности их организации по таким вопросам.

162. **Отсутствие механизма передачи, получения и перенаправления киберинформации в системе.** Точно так же должны быть созданы внутренние механизмы получения киберинформации от государств, однако инспекторы не смогли установить очевидных механизмов такого рода в ходе своего анализа. Некоторые собеседники дали понять, что среди взаимодействующих с ними государственных органов имеется некоторая путаница в отношении того, к какой организации следует обращаться, когда кибератака, обнаруженная на уровне государства, выявила связь с одной или несколькими организациями системы Организации Объединенных Наций, и какой канал связи следует использовать. Было высказано предположение, что такая информация часто имеется и может быть передана, но нет механизма надежной передачи и перенаправления ее соответствующим получателям внутри системы, в частности потому, что внешним организациям неясно, какой организации системы Организации Объединенных Наций может касаться информация. Это, в свою очередь, приводило в прошлом к упущенным возможностям защиты и ограждения ресурсов организации от атак, поскольку нельзя было гарантировать, что такая киберинформация дойдет до получателя, обладающего необходимыми знаниями, необходимыми для того, чтобы на ее основе принимать меры. Таким образом, установленные дипломатические каналы связи не считались достаточно эффективными, что приводило к упущенным возможностям в области кибербезопасности для отдельных организаций и системы в целом.

163. **Желательность и целесообразность согласованного подхода.** Некоторые из факторов, ведущих к нынешней неединообразной практике сотрудничества организаций системы Организации Объединенных Наций с национальными властями, рассмотрены в пунктах 35–37 выше. Возникает вопрос, могут ли связанные с этим несоответствия создать дополнительные проблемы, включая потенциальные репутационные риски при поддержании отношений со страной пребывания, особенно в тех случаях, когда несколько организаций системы Организации Объединенных Наций с разными подходами к вопросу имеют штаб-квартиру или отделение в одной стране, поддерживая — или не поддерживая — контакт по вопросам кибербезопасности с одними и теми же органами. **Инспекторы просят Комитет высокого уровня по вопросам управления коллективно обдумать вопрос о необходимости и целесообразности согласованного подхода к такому сотрудничеству и разработке соответствующих руководящих указаний на этот счет.** Специальная группа по информационной безопасности, Межучрежденческая сеть обеспечения безопасности и Сеть юрисконсультов имеют необходимые возможности для того, чтобы, используя свой специальный опыт, совместно изучить этот вопрос и возможности повышения безопасности, связанные с этим проблемы и, в частности, целесообразность назначения в организациях контактных лиц, в том числе на уровне системы, для передачи, получения и перенаправления информации о киберугрозах и рисках. Принимая во внимание, что Международный вычислительный

[55] The United Nations Security Management System Security Policy Manual, sect. D – Relations with host countries on security issues, para. 14(d), “Crisis management”.

центр Организации Объединенных Наций участвует в Межучрежденческой сети обеспечения безопасности, инспекторы отметили, что Центр выразил готовность играть роль в консолидации и передаче информации о киберинцидентах национальным властям от имени организаций системы Организации Объединенных Наций, если ему будет официально поручена такая роль. Хотя предоставление информации и сотрудничество с национальными властями входит в компетенцию каждой организации, то, что Международный вычислительный центр Организации Объединенных Наций имеет доступ к информации, которая позволяет ему определять связи и потенциальные взаимозависимости между атаками на различные организации, которые, как можно допустить, ни одна из организаций не могла бы вывести самостоятельно, представляет собой довод в пользу повышения роли Центра в таких вопросах и заслуживает изучения. Поэтому при рассмотрении возможности согласованного подхода в этой области соответствующим межучрежденческим механизмам следует также запрашивать и изучать потенциальные вклады соответствующих заинтересованных сторон, включая Международный вычислительный центр Организации Объединенных Наций, особенно в том, что касается способности последнего собирать, сопоставлять и анализировать данные о кибервторжениях от имени системы.

164. **Цель более тесного согласования соображений физической безопасности и кибербезопасности.** В более общем плане, поскольку руководящие принципы информационной безопасности 1992 года, разработанные предшественником Сети по цифровизации и технологиям, уже затрагивали связи между безопасностью информационных систем и физической безопасностью[56] и этот вопрос снова всплыл в ходе обсуждения в соответствующих органах в 2013–2014 годах[57], инспекторы считают своевременным возобновить усилия по более тесному согласованию функций физической безопасности и кибербезопасности для обеспечения максимально возможной защиты от многосоставных угроз. Департамент охраны и безопасности, являясь центральным нормоустанавливающим органом всей системы, призван сыграть решающую роль в признании существующих точек сближения и может существенным образом способствовать такому значительному сдвигу в организационной культуре. В этой связи в системе Организации Объединенных Наций угрозы для физической безопасности уже воспринимаются чрезвычайно серьезно, и нет никаких сомнений в необходимости незамедлительно и действенно устранять физические угрозы. Хотя инспекторы выявили чувство осторожной эволюции мышления организаций в сторону понимания необходимости такого же подхода к киберугрозам, необходимо сделать больше, чтобы распространить уже ставший преобладающим подход, основанный на оценке рисков, и структурированные, ориентированные на подотчетность меры реагирования Департамента охраны и безопасности в физической области на киберсферу. Это не означает, что общесистемный мандат, уже возложенный на Департамент охраны и безопасности, должен быть пересмотрен и теперь включать кибербезопасность. Инспекторы признают, что для решения современных проблем, создаваемых акторами киберугроз, требуются ресурсы и конкретный опыт, которых у Департамента охраны и безопасности в настоящее время нет, и что передача какой-либо части ответственности в этом вопросе будет невозможна без значительной коррекции. Любой шаг в этом направлении потребует структурных изменений, включая решения Генеральной Ассамблеи и широкие внутренние консультации и координацию с различными заинтересованными сторонами системы обеспечения безопасности Организации Объединенных Наций, в том числе по аспектам, касающимся необходимых административных и финансовых ресурсов, а также необходимости профессионального совершенствования персонала безопасности, как показано в других разделах настоящего доклада. В настоящее время обзор показывает, что общесистемные дискуссии по этому вопросу еще не вызрели и выиграют от возобновления усилий и более тщательного изучения, основанного на опыте,

[56] Information System Security Guidelines for the United Nations Organizations.

[57] CEB/2013/5, п. 40; девятнадцатая сессия Межучрежденческой сети обеспечения безопасности (2013 год, документ без условного обозначения) и двадцатая сессия Межучрежденческой сети обеспечения безопасности (2014 год, документ без условного обозначения).

имеющемся в системе, особенно на уровне Межучрежденческой сети обеспечения безопасности и Специальной группы по информационной безопасности. Поэтому инспекторы рекомендуют Генеральному секретарю изучить возможности дальнейшего использования сближения между физической безопасностью и кибербезопасностью в системе Организации Объединенных Наций и изучить преимущества и недостатки возможных способов достижения этой цели. Доклад Генеральной Ассамблее по этому вопросу должен, насколько это возможно, основываться на итогах консультаций, которые должны быть проведены между соответствующими межучрежденческими координационными механизмами, занимающимися вопросами кибербезопасности, и Межучрежденческой сетью обеспечения безопасности при необходимом вкладе Международного вычислительного центра Организации Объединенных Наций.

165. Ожидается, что выполнение следующей рекомендации повысит эффективность реагирования системы Организации Объединенных Наций на угрозы в области кибербезопасности.

Рекомендация 5

Генеральному секретарю следует представить Генеральной Ассамблее Организации Объединенных Наций не позднее ее семьдесят восьмой сессии доклад об изучении дальнейших возможностей использования сближения физической безопасности и кибербезопасности в целях обеспечения более комплексной защиты персонала и ресурсов Организации Объединенных Наций, определяющий необходимые меры по соответствующему укреплению имеющихся структур, с уделением особого внимания возможной роли Департамента охраны и безопасности в этой связи.

Приложение I

Межправительственные направления работы по кибербезопасности и киберпреступности

Введение и употребляемые термины

Вопросы, связанные с кибербезопасностью, обсуждались международным сообществом на нескольких межправительственных форумах.

С одной стороны, эта тема изучалась различными комитетами Генеральной Ассамблеи и органами, подчиняющимися ей или иным образом связанными с ней. Одним из направлений работы была определена киберпреступность (в начале 1990-х годов называвшаяся «компьютерными преступлениями»), а другим — информация и телекоммуникации в аспекте международной безопасности (включая безопасность ИКТ и связанные с ней темы).

С другой стороны, мандаты нескольких участвующих организаций затрагивают аспекты кибербезопасности, которые регулируются межправительственными процессами, поддерживаемыми этими организациями, например МСЭ, Управлением по вопросам разоружения, УНП, ВОИС, ПРООН, ЮНКТАД и МАГАТЭ.

Термины «киберпреступность» и «кибербезопасность» не взаимозаменяемы, хотя они рассматривают одну и ту же проблему с разных сторон. Можно сказать, что киберпреступность затрагивает главные аспекты совершения кибератак и уголовной ответственности злоумышленников за их участие (с использованием или в среде информационных технологий) в противоправных деяниях. Наоборот, кибербезопасность связана с защитой от таких атак, ставя в центр внимания цель и средства ее защиты, а не исполнителя атаки.

В настоящем приложении представлен обзор различных направлений межправительственной работы на уровне организаций системы Организации Объединенных Наций, их происхождения и текущей работы, а также взаимоотношений между ними, если те имеются.

Направление работы I: киберпреступность

Киберпреступность в глобальной повестке дня с 1990-х годов. Первый документально подтвержденный факт осознания международным сообществом необходимости уделения особого внимания киберизмерению программной работы, а также вложений в потенциал государств отражать кибератаки (при технической помощи со стороны соответствующих организаций системы Организации Объединенных Наций) относится еще к 1990 году и первоначально возник в связи с борьбой с международной преступностью. В частности, в своей резолюции 45/121 Генеральная Ассамблея одобрила рекомендации восьмого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями и, в частности, резолюцию о компьютерных преступлениях, в которой к государствам был обращен призыв активизировать свои усилия по более действенной борьбе с компьютерными правонарушениями. Работа над темой продолжается под рубрикой «Противодействие использованию информационно-коммуникационных технологий в преступных целях»[1] в Третьем комитете Генеральной Ассамблеи (Комитете по социальным, гуманитарным и культурным вопросам) и под рубрикой «киберпреступность» в Комиссии по предупреждению преступности и уголовному правосудию (функциональной комиссии

[1] Резолюции 73/187, 74/247 и 75/539 Генеральной Ассамблеи и более ранние резолюции 55/63 и 56/121.

Экономического и Социального Совета). Основную и административную поддержку ей оказывает УНП.

Текущая работа над международной конвенцией о киберпреступности. Усилия по проведению «всестороннего исследования проблемы киберпреступности» продолжаются с 2010 года в рамках межправительственной экспертной группы открытого состава (или «МГЭ по киберпреступности»), созданной с этой целью под эгидой Комиссии по предупреждению преступности и уголовному правосудию[2]. Работа, проделанная в результате, набрала импульс и придала толчок отдельным усилиям по разработке обязательного правового акта о киберпреступности. Процессом разработки и переговоров по этому правовому акту руководит специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно- коммуникационных технологий в преступных целях (называемый «специальным комитетом»), который был учрежден Генеральной Ассамблеей в 2019 году и начал свою работу в 2020 году[3]. Конечный результат этого процесса должен быть представлен главным образом государствам как участникам итоговой конвенции. Правовая основа, которую предполагается выработать, в основном предназначена для регулирования обращения с правонарушителями (киберпреступниками) на уровне государств и поэтому имеет мало прямого отношения к подходу организаций системы Организации Объединенных Наций к кибербезопасности. Поэтому связанные с этим усилия не представляют большого интереса для настоящего обзора.

Направление работы II: информация и телекоммуникации в контексте международной безопасности

Второе направление межправительственной работы, «рассмотрение существующих и потенциальных угроз в области информационной безопасности», с 1998 года стало фигурировать в резолюциях Генеральной Ассамблеи в рамках недавно внесенного и с тех пор повторяющегося пункта повестки дня, «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[4]. Этой темой занимались два межправительственных органа, действующих в рамках Первого комитета (Комитета по разоружению и международной безопасности) Генеральной Ассамблеи: a) Группа правительственных экспертов — орган, состоящий из ограниченного числа экспертов, назначенных Генеральным секретарем и действующих в своем личном качестве[5], в настоящее время шестая подобная группа с момента создания первой такой Группы в 2004 году[6]; и b) Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (открыта для всех государств — членов Организации Объединенных Наций, создана в 2018 году)[7]. Основные задачи обеих групп — «рассмотрение существующих и потенциальных угроз в сфере информационной безопасности и возможные совместные меры по их устранению»[8] и «дальнейшее развитие правил, норм и принципов ответственного поведения государств [перечисленных в резолюции] и способов их реализации»[9]. Рабочая группа открытого состава и шестая Группа правительственных экспертов завершили свою работу и, соответственно, в марте и мае 2021 года приняли консенсусом свои доклады[10]. Ожидается, что недавно созданная новая Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий в период 2021–2025 годов рассмотрит работу своей предшественницы (которая

[2] Резолюция 65/230 Генеральной Ассамблеи.
[3] Резолюция 74/247 Генеральной Ассамблеи.
[4] См. резолюцию 53/70 Генеральной Ассамблеи и последующие резолюции, последней из которых является резолюция 75/240.
[5] См. резолюцию 58/32 Генеральной Ассамблеи.
[6] См. резолюцию 73/226 Генеральной Ассамблеи.
[7] См. резолюцию 73/27 Генеральной Ассамблеи.
[8] См. резолюцию 58/32 Генеральной Ассамблеи, п. 4.
[9] См. резолюцию 73/27 Генеральной Ассамблеи.
[10] См. A/75/816.

охватывала период 2019–2020 годов), и впервые соберется в 2021 году[11]. Оперативно-функциональным обеспечением работы этих органов занимается Управление Организации Объединенных Наций по вопросам разоружения.

Мандаты организаций системы Организации Объединенных Наций в области кибербезопасности

Мандаты ряда организаций системы Организации Объединенных Наций в области основного и технического сотрудничества касаются аспектов кибербезопасности. Одним из примеров — МСЭ, который, среди прочего, принимает у себя ежегодный форум Всемирной встречи на высшем уровне по вопросам информационного общества, который является основным механизмом решения проблемы ИКТ в целях развития и единственным координатором направления действий С5 Всемирной встречи на высшем уровне по вопросам информационного общества, «Укрепление доверия и безопасности при использовании ИКТ». В этой роли МСЭ работает с ключевыми заинтересованными сторонами, чтобы помочь странам, в числе прочего, принять национальные стратегии кибербезопасности, расширить возможности государств по реагированию на инциденты, внедрить международные стандарты безопасности, защитить детей в сети и создать потенциал. Часть работы, проделанной в рамках Всемирной встречи на высшем уровне по вопросам информационного общества, упоминается в резолюциях Генеральной Ассамблеи «Создание глобальной культуры кибербезопасности», подготовленных во Втором комитете Генеральной Ассамблеи (Комитете по экономическим и финансовым вопросам)[12]. Другие организации с мандатами, охватывающими аспект кибербезопасности, — это УНП, ВОИС, ПРООН, ЮНКТАД, Управление по вопросам разоружения и МАГАТЭ, а также в той или иной степени многие другие.

Подборка мандатов и основных мероприятий организаций системы Организации Объединенных Наций в области кибербезопасности и киберпреступности, составленная в рамках КСР, была призвана обрисовать все способы, которыми эти организации участвовали в рамках их соответствующих мандатов и направлений деятельности в оказании технической помощи и поддержки в разработке политики в этой области на протяжении ряда лет. Однако подборка осталась внутренним документом, доработка и обновление которого оказались чересчур монументальной задачей. Она служит убедительным подтверждением разнообразия и фрагментации программной работы организаций системы Организации Объединенных Наций по этому вопросу. В этой связи Комитет высокого уровня по программам неоднократно заявлял о необходимости применения в системе скоординированного и последовательного подхода с учетом взаимодополняющего характера, а также степени совпадения соответствующих мандатов каждой организации[13].

[11] См. резолюцию 75/240 Генеральной Ассамблеи.

[12] Резолюции 57/239 и 64/211 Генеральной Ассамблеи.

[13] См., например, CEB/2010/HLCP-XX/CRP.7, п. 3; CEB/2010/6, пп. 38–43; CEB/2011/HLCP-XXII/CRP.6; CEB/2014/6, пп. 42–49.

Приложение II

Некоторые элементы подхода к кибербезопасности, основанного на оценке рисков

Помимо официального включения кибербезопасности в общеорганизационный реестр рисков или матрицу рисков организации, инспекторы хотят выделить три аспекта подхода к кибербезопасности, основанного на оценке рисков, который может ускорить получение соответствующих преимуществ: a) индивидуальный, систематический и адаптивный подход к оценке рисков; b) официально объявленная на высоком уровне допустимая степень риска; c) адекватные возможности для специалистов по кибербезопасности использовать свои знания в процессе управления рисками; и d) использование тестирования на проникновение в качестве инструмента управления рисками.

- **Индивидуализированная оценка рисков.** Оценка рисков кибербезопасности должна учитывать условия деятельности организации при должном учете таких критериев, как ее полномочия, финансовые и кадровые возможности, бизнес-модель, характер используемой или хранящейся информации и особенности организации, такие как возможное влияние киберинцидентов на осуществление возложенных функций, в том числе в условиях децентрализации или географической рассредоточенности отделений. Некоторые участвующие организации ссылаются на отраслевые стандарты в обоснование своего процесса оценки рисков, что можно считать передовой практикой при условии, что названные стандарты сами выбираются исходя из того, насколько хорошо они соответствуют контексту данной организации (пп. 59–64). Помимо индивидуализации оценок рисков, следует выделить аспект периодичности, который не только способствует систематическому подходу, но и обеспечивает адаптируемость структуры и, в идеале, оперативность реагирования на постоянно меняющийся ландшафт угроз, который может не совпадать с циклами регулярного обзора.

- **Официально объявленная допустимая степень риска.** Одним из основных элементов более стратегического подхода к управлению рисками кибербезопасности является официальное указание о допустимой степени риска, в идеале подготовленное при участии директивных и руководящих органов, а также исполнительного руководства организации (пп. 53–54). Официальное решение о допустимой степени риска целесообразнее всего строить на всесторонней периодической оценке рисков для кибербезопасности, охватывающей все категории угроз для кибербезопасности, а не только угрозы конфронтационного характера или угрозы, внешние по отношению к организации (пп. 25–29), и на информации о состоянии общеорганизационных информационных систем и известных уязвимостях, полученной как от подразделения ИКТ, так и от оперативных подразделений в духе общеорганизационного подхода. Определение допустимой степени риска приобретает первостепенное значение, если оно основано на тщательно отобранном и разработанном наборе значимых показателей кибербезопасности. Это зависящий от специфики каждой организации процесс, который будет определять дальнейшие управленческие решения, такие как создание внутреннего (в отличие от внешнего) общеорганизационного потенциала кибербезопасности; выделенные ему ресурсы; инструменты и политические рекомендации, включенные в нормативную базу; а также решения об инвестициях и реагировании на инциденты в случае их доведения до сведения руководства. В таких организациях, как ВОИС и МАГАТЭ, которые оперируют с особо конфиденциальной информацией, допустимая степень риска по определению может быть низкой. Допустимые для организации пределы риска могут также уменьшиться в результате происшедших в прошлом серьезных киберинцидентов, что, однако чревато опасностью чрезмерного

инвестирования в киберзащиту, которая, в свою очередь, может создать ложное ощущение безопасности.

- **Опыт в области кибербезопасности, используемый в процессах управления рисками.** Предоставление надлежащих возможностей использования опыта в области кибербезопасности в общеорганизационных процессах управления рисками может показаться очевидным, но во многих организациях это далеко от реальности. Формат и периодичность соответствующих вводимых данных не имеют решающего значения, но важна надежная (беспрепятственная и не разовая) форма доступа специалистов по кибербезопасности к центрам решений об управлении рисками в организации, и ее следует вводить систематически, чтобы гарантировать что критические соображения кибербезопасности получают отражение на этапах концептуализации, осуществления и контроля системы менеджмента рисков организации. В некоторых организациях, в которых существует должность главного сотрудника по информационной безопасности, тот состоит членом комиссии по общеорганизационному управлению рисками или стал его официальным членом или приглашается к участию в ее работе. Полученные отзывы о такой схеме были положительными, и, возможно, стоит внедрить ее в практику во всех организациях.

- **Тестирование на проникновение как инструмент управления рисками.** Тестирование на проникновение (часто сокращенно «пентест») — это санкционированная имитация реальной атаки, нацеленной на сети, системы и людские ресурсы организаций с использованием инструментов и методов, обычно применяемых злоумышленниками, с целью выявления уязвимостей в средствах защиты организации, оценки эффективности предусмотренных мер противодействия и отработки процедур реагирования и устранения последствий. Тестирование на проникновение в основном проводится внешними подрядчиками в соответствии с правилами, разработанными для обеспечения индивидуализированной и реалистичной оценки, при сведении к минимуму возможности серьезного ущерба для ресурсов и процессов организации. Несколько участвующих организаций используют этот способ, в некоторых случаях привлекая разных (например, чередующихся) подрядчиков в течение определенного периода времени, в идеале с разной специализацией, чтобы атаковать организацию (команда «красных») и проверить готовность защиты (команда «синих»). Одна организация выбрала способ, когда внешнему подрядчику (имитировавшему атаку) противостояли специалисты его центра обеспечения безопасности (отражавшему ее), что позволило обеим командам взаимодействовать в реальном времени по поводу результатов и возможных действий по преодолению последствий (группа «фиолетовых»). Независимо от того, используется ли при этом один подрядчик или несколько подрядчиков, тестирование на проникновение — сложное мероприятие, требующее основательной подготовки и тщательного отбора заслуживающих доверия экспертов, оценивающих состояние систем (и выступающих в качестве злоумышленников), поскольку имеются реальные риски, связанные с предоставлением даже временного допуска к закрытым системам и информации. Однако это продвинутый и действенный инструмент управления рисками, который можно использовать для поддержки планирования бесперебойности деятельности, и надежный метод быстрого получения представления о состоянии кибербезопасности в организации с различных точек зрения, выявления брешей в ее общей защите или конкретных уязвимости в отдельных областях в зависимости от заранее заданного масштаба такой оценки.

Приложение III

Основные отраслевые стандарты, используемые организациями — участницами Объединенной инспекционной группы

ИСО 27001 (Международная организация по стандартизации, 2005 год)[1]

Стандарт ИСО 27001, используемый в основном для аудита и проверки соответствия, в первую очередь рассматривает то, что должно быть достигнуто в технических областях защиты кибербезопасности и содержит соответствующие рекомендации. Стандарт использует общий набор из 14 элементов управления, направленных на отражение кибербезопасности в целях деятельности организации и методах управления рисками. Его основные группы управления охватывают правила информационной безопасности, управление активами, контроль доступа, безопасность деятельности и связи, действия в случае инцидента и соблюдение требований. Благодаря ее особенностям стандарт, по-видимому, лучше всего подходит для анализа и аудита мер кибербезопасности в более крупных организациях, хорошо обеспеченных ресурсами.

Рекомендации Национального института стандартов и технологий Соединенных Штатов, созданного в 1901 году[2]

Определяя цели и приоритеты организации и организуя соответствующие действия, Национальный институт стандартов и технологий Соединенных Штатов дает гибкие и адаптируемые рекомендации для понимания рисков кибербезопасности. В дополнение к внутренним руководящим положениям, рекомендации, последний раз обновлявшиеся в 2015 году, также увязаны с другими стандартами, руководящими принципами и практикой, такими как рекомендации Центра интернет-безопасности, международные стандарты Международной организации по стандартизации, Цели контроля для информационных и связанных технологий и т. п. План действий Национального института стандартов и технологий определяет пять основных функций (идентификация, защита, обнаружение, реагирование и восстановление) и классифицирует потоки информации и решений по различным уровням внутри организации. Благодаря в высшей степени целостному подходу этот стандарт, по-видимому, особенно хорошо подходит для определения стратегий и политики кибербезопасности организации.

Цели контроля для информационных и связанных технологий (Ассоциация аудита и контроля информационных систем (АУКИС), 1996 год)[3]

Цели контроля для информационных и связанных технологий, система стандартов для руководства и управления информационными технологиями, основаны на передовых методах, которые помогают организациям достигать своих целей в области соблюдения нормативных требований и управления рисками, а также согласовывать свою стратегию информационных технологий со своими целями. В концептуальном плане этот стандарт основан на концепции уровней возможностей с упором на адаптации услуг в соответствии с потребностями организации. В соответствии с этим международным стандартом аспекты информационной безопасности относятся к категории управления рисками и обеспечения непрерывности и доступности бизнес-услуг. В дополнение к внутренним материалам Цели контроля для информационных и связанных технологий увязаны с другими стандартами и рекомендациями, включая рекомендации Национального института стандартов и технологий Соединенных Штатов, ИСО 27001 и рекомендации Центра

[1] URL: www.iso.org/home.html.
[2] URL: www.nist.gov.
[3] URL: www.isaca.org/credentialing/cobit/cobit-foundation.

контроля интернет-безопасности. Задачи согласования, содержащиеся в этом стандарте, которые в наибольшей степени относятся к данной теме, включают управление рисками информационных технологий, информационную безопасность, соответствие нормативным требованиям, а также непрерывность и доступность бизнес-услуг. Что касается рекомендаций по кибербезопасности, то стандарт, по-видимому, лучше всего подходит для организаций, которые уже используют Цели контроля для информационных и связанных технологий в своей структуре руководства и управления ИКТ. Кроме того, этот критерий можно расширить, объединив его с другими стандартами, к которым он дает отсылки (Центр интернет-безопасности, рекомендации Национального института стандартов и технологий и ИСО 27001).

Библиотека инфраструктуры информационных технологий (Центральное управление вычислительной техники и связи Соединенного Королевства Великобритании и Северной Ирландии, 1980-е годы)[4]

Библиотека инфраструктуры информационных технологий представляет собой набор рекомендаций по управлению услугами ИКТ и включает серию публикаций, содержащих соответствующие рекомендации по предоставлению услуг ИКТ, а также по необходимым процессам и ресурсам, которые требуются организациям. Стандарт, разработанный Центральным управлением вычислительной техники и связи Соединенного Королевства в 1980-х годах, представляет собой серию из пяти томов, каждый из которых охватывает различные фазы цикла управления услугами ИКТ. Основные темы включают определение стоимости услуг, развитие деятельности, вспомогательные активы, анализ рынка и виды поставщиков услуг. С 2005 года практика Библиотеки инфраструктуры информационных технологий внесла свой вклад в стандарт ИСО 20000 и согласовала его с ним.

Стандарт Центра интернет-безопасности, 2008 год[5]

Стандарт, также известный как Критические меры контроля кибербезопасности, представляет собой набор рекомендаций, основанных на отраслевом передовом опыте. Несмотря на то что он имеет в первую очередь техническую ориентацию, стандарт Центра интернет-безопасности также включает несколько мер контроля, касающихся более широких организационных аспектов кибербезопасности, таких как обучение по вопросам информированности и реагирование на инциденты. Стандарт представляется довольно практичным и крайне полезным в плане групп реализации, рассматривая действия, которые необходимо реализовать в соответствии с размерами организации, кадрами, имеющимися ресурсами и степенью конфиденциальности данных. Его основные меры контроля включают имущество и ресурсы, защиту от уязвимостей, безопасность конфигурации, защиту электронной почты и веб-браузера, восстановление и защиту данных, реагирование на инциденты и тестирование на проникновение. Такой подход оказался особенно подходящим для реализации стратегий защиты кибербезопасности в малых и средних организациях с уже существующими системами менеджмента рисков, которые включают аспекты кибербезопасности.

[4] URL: www.axelos.com/best-practice-solutions/itil.
[5] URL: www.cisecurity.org/controls/.

Приложение IV

Нормативно-правовая база организаций системы Организации Объединенных Наций в области кибербезопасности

a) Уровни нормативной базы кибербезопасности

Стратегический уровень	Часто один документ, содержащий указания руководства в общих терминах	Определяет организационное видение, цели и общие принципы, излагает основные принципы управления, организационные роли и обязанности, а также может сформулировать кибербезопасность как организационное решение, включая указания о допустимой степени риска	Относится к общеорганизационному уровню, в основном предназначен для его осуществления высшим руководством
Уровень политики	Серия отдельных документов, содержащих предписывающие, требующие действий формулировки, обычно публикуемых в виде официальных административных бюллетеней	Определяет организационные принципы, лежащие в основе системы обеспечения информационной безопасности, с обязательными внутренними положениями и правилами, определяющими цели и связанные с ними меры, организованными по темам (например, классификация информации, управление рисками, непрерывность деятельности и восстановление после аварии, а также допустимое использование данных и ресурсов ИКТ) и устанавливающими конкретные функции и обязанности	Относится ко всему персоналу и подразумевает возможность дисциплинарных взысканий в случае несоблюдения
Процедурный уровень	Серия руководящих указаний или типовых порядков действий, поддерживающих директивы более высокого уровня, с описанием процессов, направленных на установление систематической практики	Предоставляет подробные инструкции по конкретным шагам, которые следует предпринять, или действиям, которых следует избегать (соблюдение правил использования паролей, регулярное антивирусное сканирование и обновление ПО, сканирование USB-накопителей (с интерфейсом «универсальная последовательная шина»), полученных в подарок, перед их использованием; и т. д.)	Может применяться ко всему персоналу или быть ориентированным на определенные роли (например, персонал ИКТ, архивисты и документоведы, а также специалисты по закупкам)
Технический уровень	Серия технических протоколов, направленных на правильное и единообразное исполнение	Излагают подробные пошаговые инструкции, требующие больших познаний в предметной области для применения и реализации. Темы могут включать, среди прочего, конфигурацию базы данных, безопасность сети и безопасность облачной среды	В основном адресованы техническим специалистам

Источник: Подготовлено ОИГ.

b) Стратегии в области информационно-коммуникационных технологий и специальные документы по политике в области кибербезопасности в участвующих организациях

Участвующая организация	*Организационная стратегия в области информационных и коммуникационных технологий с элементом кибербезопасности*	*Специальные документы по политике кибербезопасности*
Секретариат Организации Объединенных Наций	Да, информационно-коммуникационные технологии в Организации Объединенных Наций (A/69/517) и резолюция 69/262 Генеральной Ассамблеи)	Да, Директива о правилах информационной безопасности для Секретариата Организации Объединенных Наций (2013 год)
ЮНЭЙДС	Нет, Стратегия в области ИКТ (2017–2020 годы) не включает кибербезопасность	Нет, ЮНЭЙДС работает над глобальным планом кибербезопасности, который также будет охватывать правила кибербезопасности
ЮНКТАД	Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно-коммуникационных технологий	Да, соответствует Стратегии кибербезопасности Секретариата Организации Объединенных Наций
ПРООН	Да, Стратегия информационных технологий (на 2020–2023 годы)	Да, Правила информационной безопасности (2016 год)
ЮНЕП	Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно-коммуникационных технологий	Да, соответствует Стратегии кибербезопасности Секретариата Организации Объединенных Наций
ЮНФПА	Да, Стратегия в области информационно-коммуникационных технологий (2018–2021 годы)	Да, Правила безопасности информационно-коммуникационных технологий
Хабитат ООН	Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно-коммуникационных технологий	Да, соответствует Стратегии кибербезопасности Секретариата Организации Объединенных Наций
УВКБ	Да, Стратегия информационных технологий (2020–2022 годы) (окончательный проект находится на рассмотрении)	В настоящее время разрабатывается
ЮНИСЕФ	Да, Стратегия информационно-коммуникационных технологий	Да, Стратегический план ЮНИСЕФ по информационной безопасности (2018–2022 годы)
УНП/ЮНОВ	Соответствует стратегии Секретариата Организации Объединенных Наций в области информационно-коммуникационных технологий	Да, соответствует Стратегии кибербезопасности Секретариата Организации Объединенных Наций
ЮНОПС	Пятилетняя стратегия в области ИКТ (в стадии разработки)	Да, информационная безопасность
БАПОР	Да, стратегия управления информацией (2019–2020 годы)	Имеется отдельная стратегия информационной безопасности (ожидает окончательного утверждения)
ООН-женщины	Да, Стратегия в области информационных и коммуникационных технологий (2018–2021 годы)	Да, Правила информационной безопасности
ВПП	Да, Общеорганизационная стратегия информационных технологий (2016–2020 годы)	Да, Общеорганизационные правила безопасности информации и информационных технологий (2015 год)

Участвующая организация	*Организационная стратегия в области информационных и коммуникационных технологий с элементом кибербезопасности*	*Специальные документы по политике кибербезопасности*
ФАО	Да, Цифровая стратегия информационно-коммуникационных технологий (2017 год)	Да, Правила информационной безопасности
МАГАТЭ	Да, Стратегический план производственных технологий (2015–2020 годы)	Да, Стандарты информационной безопасности
ИКАО	Да, Цифровая стратегия информационно-коммуникационных технологий (2017 год) (на рассмотрении)	Да, Правила информационной безопасности (2007 год, 2-я редакция)
МОТ	Да, Стратегия информационных технологий (2018–2021 годы)	Да, Правила информационной безопасности электронных систем (2010 год)
ИМО	Да, Стратегический план в области информационно-коммуникационных технологий (2019–2023 годы)	Да, Управление рисками информационной безопасности (2015 год)
МСЭ	Нет, МСЭ применяет более целостный подход к внедрению системы управления организационной устойчивостью, включая разработку подробного анализа воздействия на деятельность, отображающего стратегические риски и стратегии воздействия на деятельность, а также антикризисное управление, обеспечение бесперебойности деятельности и послеаварийное восстановление ИКТ	Нет
ЮНЕСКО	Да, Стратегия управления знаниями и информационно-коммуникационных технологий (2018–2021 годы)	Да, включена в систему общеорганизационного управления рисками и Сборник должностных инструкций (правила безопасности информации и информационных технологий)
ЮНИДО	Стратегия корпоративных информационно-коммуникационных технологий (2029–2021 годы)	Нет
ЮНВТО	Нет, Стратегия информационно-коммуникационных технологий не охватывает кибербезопасность	Нет, в стадии разработки
ВПС	Нет, стратегия ВПС в области ИКТ будет подготовлена в декабре 2021 года	Нет
ВОЗ	Да, Стратегия в области управления информацией и технологий (2019 год)	Да, Стратегия кибербезопасности
ВОИС	Да, Стратегия информационно-коммуникационных технологий (новая стратегия находится в стадии разработки)	Да, Правила и стандарты информационной безопасности и Стратегия информационной безопасности нового поколения (2021–2024 годы)
ВМО	Да, Стратегия в области информационных и коммуникационных технологий (2020–2023 годы)	Нет

Приложение V

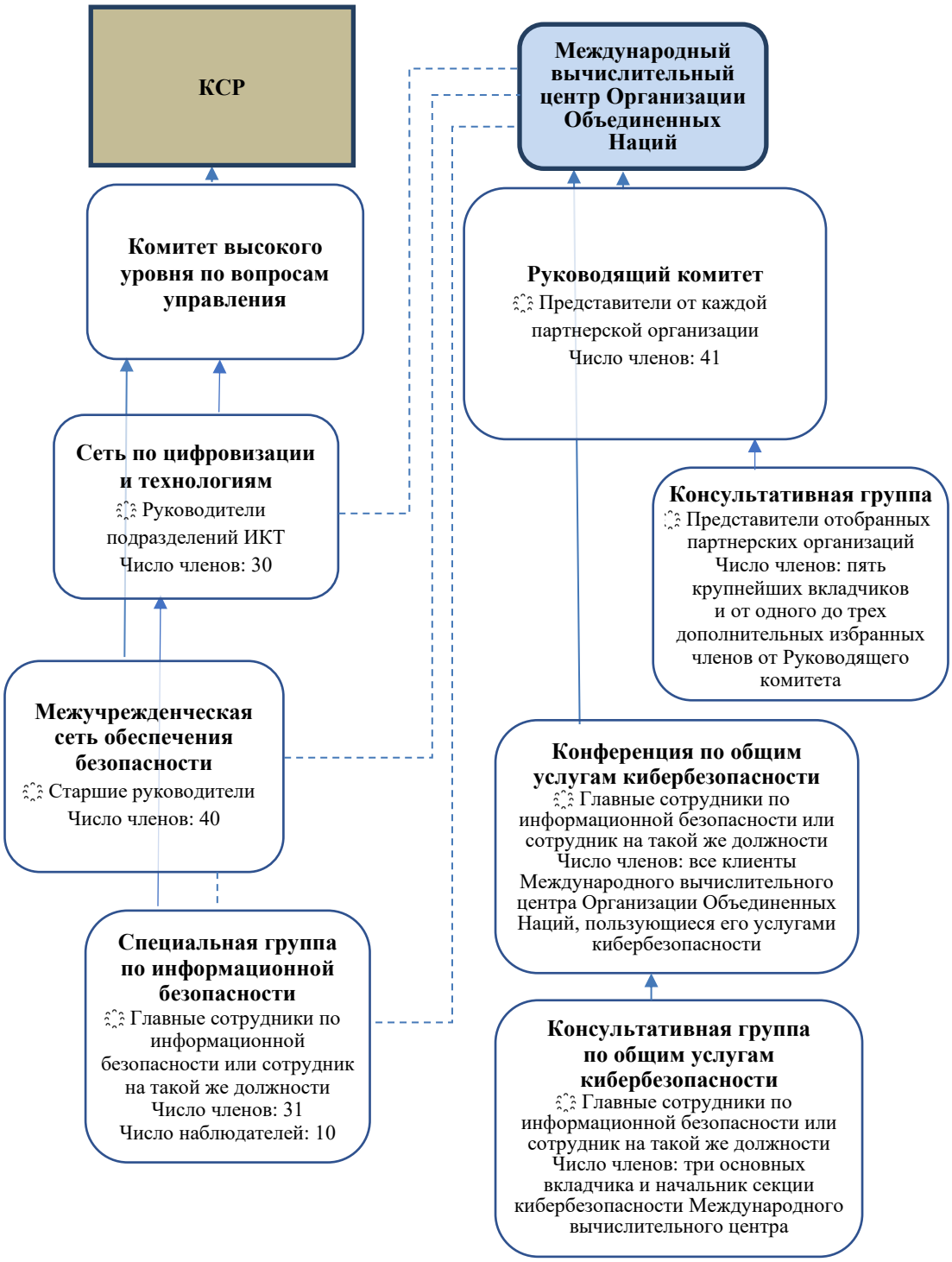
Механизмы кибербезопасности и их место в иерархической структуре организаций — участниц Объединенной инспекционной группы на январь 2021 года

Участвующая организация	*Вопросы кибербезопасности решаются предназначенным для этой цели или специализированным штатным подразделением*	*Кибербезопасность обеспечивается подразделением ИКТ организации (среди его других функций)*	*Используется «главный сотрудник по информационной безопасности как услуга» или услуга управления безопасностью, предоставляемая Международным вычислительным центром Организации Объединенных Наций*	*Подчиненность начальнику подразделения ИКТ (или сотруднику на эквивалентной должности)*
Секретариат Организации Объединенных Наций	√		X	√
ЮНЭЙДС		√	X	√
ЮНКТАД		√	√ (Нынешний клиент)	√
ПРООН	√		X	√
ЮНЕП		√	X	√
ЮНФПА	√ (Начата процедура назначения главного сотрудника по информационной безопасности)	√ (Вплоть до завершения процедуры назначения)	√ (Нынешний клиент)	√
УВКБ	√		X	√
ЮНИСЕФ	√		√ (Нынешний клиент)	√
УНП/ЮНОВ		√	X	√
ЮНОПС	√		X	Главный сотрудник по информационной безопасности подчиняется главному финансовому сотруднику и директору администрации
БАПОР	√		X	√
ООН-женщины		√	√ (Прошлый клиент)	√
ВПП	√		√ (Прошлый клиент)	√
ФАО	√		√ (Нынешний клиент)	√

Участвующая организация	*Вопросы кибербезопасности решаются предназначенным для этой цели или специализированным штатным подразделением*	*Кибербезопасность обеспечивается подразделением ИКТ организации (среди его других функций)*	*Используется «главный сотрудник по информационной безопасности как услуга» или услуга управления безопасностью, предоставляемая Международным вычислительным центром Организации Объединенных Наций*	*Подчиненность начальнику подразделения ИКТ (или сотруднику на эквивалентной должности)*
МАГАТЭ	√		X	√
ИКАО	√		√ (Прошлый клиент)	Главный сотрудник по информационной безопасности подчиняется непосредственно руководителю администрации
МОТ	√		X	√
ИМО		√	X	√
МСЭ	√		X	√
ЮНЕСКО	√		√ (Нынешний клиент)	√
ЮНИДО		√	X	√
ЮНВТО		√	X	√
ВПС		√	X	√
ВОЗ	√		√ (Прошлый клиент)	√
ВОИС	√		X	Начальник Отдела безопасности и информационного обеспечения, отвечающий одновременно за физическую и информационную безопасность, подчиняется помощнику генерального директора по вопросам администрации, финансов и управления
ВМО		√	√ (Нынешний клиент)	√

Приложение VI

Межведомственные институциональные и рабочие механизмы кибербезопасности



Источник: Подготовлено ОИГ.

Приложение VII

Услуги кибербезопасности Международного вычислительного центра Организации Объединенных Наций, используемые организациями — участницами Объединенной инспекционной группы, по состоянию на январь 2021 года

Услуги кибербезопасности	*Краткое описание*	*Число нынешних подписчиков из числа организаций — участниц Объединенной инспекционной группы*	*Число прошлых подписчиков или участников завершенных проектов из числа организаций — участниц Объединенной инспекционной группы*
Общая аналитика угроз безопасности	Постоянный и своевременный сбор информации от учреждений-членов; коммерческие фирмы по предоставлению услуг безопасности; поставщики услуг; федеральные, региональные и местные государственные органы; правоохранительные и другие авторитетные ресурсы, которые позволяют подписавшимся организациям обмениваться актуальной и конкретной информацией о любых угрозах для физической безопасности и кибербезопасности, а также любой информацией об инцидентах.	17	
Единый сервис электронной подписи	Предоставляет возможность поддержки цифровых подписей.	14	
Осведомленность об информационной безопасности	Предоставляет стратегические консультационные услуги для оказания помощи организациям в создании современной действенной стратегии осведомленности об информационной безопасности или ведущей в отрасли облачной учебной лаборатории или поддержки связи, включая информационные продукты, включая сообщения, бюллетени, плакаты и поддержку порталов.	7	3
Защита от уязвимостей	Сочетание процессов и технологий, обеспечивающих непрерывное выявление и устранение уязвимостей и изъянов конфигурации. Достигается, в частности, с помощью сканирования уязвимостей хостов и приложений, проверок безопасности конфигурации и мониторинга следа в Интернете.	6	1

Услуги кибербезопасности	*Краткое описание*	*Число нынешних подписчиков из числа организаций — участниц Объединенной инспекционной группы*	*Число прошлых подписчиков или участников завершенных проектов из числа организаций — участниц Объединенной инспекционной группы*
Службы поддержки руководителей и главного сотрудника по информационной безопасности	Служба системы обеспечения информационной безопасности, предназначенная для защиты ресурсов организации и снижения риска негативного воздействия на репутацию, потери важной информации и злонамеренных действий, а также рисков для интеллектуальной собственности, конфиденциальных данных и репутации.	6	5
Услуги моделирования фишинга	Тестируют эффективность программ повышения осведомленности об информационной безопасности организаций. Включают как разработку, так и проведение кампаний по моделированию фишинга и последующие сообщения.	6	
Служба общего центра обеспечения безопасности	Предоставляет специализированные знания для мониторинга, анализа и реагирования на события, касающиеся кибербезопасности, позволяя подписавшимся организациям своевременно реагировать на инциденты, связанные с безопасностью, используя сочетание технологических процессов и решений.	4	1
Реагирование на инциденты	Предусматривает основанные на отраслевых стандартах процедуры действий по анализу данных, связанных с инцидентами, и определения соответствующих мер реагирования на любые инциденты, связанные с безопасностью организации, в режиме реального времени.	4	7
Оценка безопасности облачной среды	Оценка, миграция, внедрение и полностью управляемая эксплуатационная поддержка, а также планирование затрат для ряда облачных решений.	4	1
Тестирование на проникновение	Позволяет выявлять слабые места в средствах контроля за информационной безопасностью и определяет масштабы возможного проникновения злоумышленников в сеть или тестируемые системы.	3	4
Общая инфраструктура открытого ключа	Поддерживает шифрование с открытым и закрытым ключом и цифровые подписи, что создает безопасную среду для электронных операций и передачи данных.	3	

Услуги кибербезопасности	*Краткое описание*	*Число нынешних подписчиков из числа организаций — участниц Объединенной инспекционной группы*	*Число прошлых подписчиков или участников завершенных проектов из числа организаций — участниц Объединенной инспекционной группы*
Управление идентификацией и доступом	Сбор, анализ и представление информации о приложениях по управлению идентификацией и доступом.	2	1
Общая информация о безопасности и действия в случае событий	Обеспечивает анализ в реальном времени тревожных оповещений, направляемых приложениями и сетевым оборудованием.	1	

Источник: Каталог услуг Международного вычислительного центра Организации Объединенных Наций (июль 2021 года) и ответы участвующих организаций на анкеты ОИГ.

Приложение VIII

Сопоставление членского состава организаций, занимающихся кибербезопасностью, по состоянию на январь 2021 года

Участвующие организации	*Сеть по цифровизации и технологиям (тридцать третья сессия, 2019 год)*	*Специальная группа по информационной безопасности (восьмой симпозиум, 2019 год)*	*Международный вычислительный центр Организации Объединенных Наций Руководящий комитет (2020 год)*	*Клиенты службы кибербезопасности Международного вычислительного центра Организации Объединенных Наций (прошлые и нынешние)*
Секретариат Организации Объединенных Наций	√	√	√	X
ЮНЭЙДС	√	X	√	X
ЮНКТАД	√	X	√	√
ПРООН	√	√	√	√
ЮНЕП	√	X	√	X
ЮНФПА	√	√	√	√
Хабитат ООН	√	X	X[1]	X
УВКБ	√	√	√	√
ЮНИСЕФ	√	√	√	√
УНП/ЮНОВ	X	X	X[2]	√
ЮНОПС	√	X	√	√
БАПОР	√	X	√	√
ООН-женщины	√	√	√	√
ВПП	√	√	√	√
ФАО	√	X	√	√
МАГАТЭ	√	√	√	√
ИКАО	√	X	√	√
МОТ	√	√	√	√
ИМО	√	X	√	√
МСЭ	√	√	√	√
ЮНЕСКО	√	X	√	√
ЮНИДО	√	√	√	√
ЮНВТО	X	√	X	√
ВПС	X	√	√	X

[1] Международный вычислительный центр Организации Объединенных Наций сообщил, что Хабитат ООН представлен в Руководящем комитете Секретариатом Организации Объединенных Наций.

[2] Международный вычислительный центр Организации Объединенных Наций сообщил, что УНП/Отделение Организации Объединенных Наций в Вене представлено в Руководящем комитете Секретариатом Организации Объединенных Наций.

Участвующие организации	*Сеть по цифровизации и технологиям (тридцать третья сессия, 2019 год)*	*Специальная группа по информационной безопасности (восьмой симпозиум, 2019 год)*	*Международный вычислительный центр Организации Объединенных Наций Руководящий комитет (2020 год)*	*Клиенты службы кибербезопасности Международного вычислительного центра Организации Объединенных Наций (прошлые и нынешние)*
ВОЗ	X	√	√	√
ВОИС	√	√	√	√
ВМО	√	√	√	√

Приложение IX

Глоссарий терминов кибербезопасности

Ботофермы, ботнет	Ботнет — это большое количество инфицированных компьютеров, которые используются для создания и рассылки спама или вирусов или наводнения сети сообщениями при атаке типа «отказ в обслуживании». *Источник*: ESCAL Institute of Advanced Technologies, glossary of security terms www.sans.org/security-resources/glossary-of-terms/
Взлом	Преднамеренное или непреднамеренное раскрытие информации, которое отрицательно сказывается на ее конфиденциальности, целостности или доступности. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary
Распределенная атака типа «отказ в обслуживании»	Атака, при которой несколько инфицированных систем используются для атаки одной цели. Поток входящих сообщений в атакуемую систему вынуждает ее выключиться и отказывать в обслуживании незлонамеренным пользователям. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary
Шифрование	Математическая функция, которая защищает информацию, делая ее нечитаемой для всех, кроме тех, у кого есть ключ для ее расшифровки. *Источник*: Национальный центр кибербезопасности (Соединенное Королевство) www.ncsc.gov.uk/information/ncsc-glossary
Оконечное устройство	Любое подключенное к сети устройство — такое, как настольные компьютеры, ноутбуки, смартфоны, планшеты, принтеры или другое специализированное оборудование, например, кассовые терминалы в торговых точках, — которое используется как пользовательская оконечная точка в распределенной сети. *Источник*: Barracuda Networks Inc., Glossary www.barracuda.com/glossary/endpoint-device
Межсетевой экран	Устройство обеспечения безопасности сети, контролирующее объем и характер входящего и исходящего сетевого трафика. Защищает локальные системные ресурсы от доступа извне. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary

Интернет вещей	Сеть разнообразных контролируемых через Интернет устройств, которые могут подключаться друг к другу и обмениваться информацией. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary
Вредоносное ПО	Вредоносное программное обеспечение, предназначенное для инфицирования или повреждения компьютерной системы без согласия владельца. Распространенные формы вредоносного ПО — компьютерные вирусы, черви, трояны, шпионское и рекламное ПО. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary
Фишинг	Попытка третьей стороны получить конфиденциальную информацию у лица, группы или организации, выдавая себя за конкретного, обычно хорошо известного отправителя сообщений, как правило с корыстными целями. Мошенники пытаются обманом заставить пользователей раскрыть личные данные, такие как номера кредитных карт, параметры доступа в систему банковского обслуживания и другую конфиденциальную информацию, которую они могут затем использовать для совершения мошеннических действий. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary
Программы-вымогатели	Тип вредоносного ПО, которое блокирует пользователю вход в систему или доступ к данным до тех пор, пока не будет выплачена денежная сумма. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary
Теневая ИТ	Оборудование или ПО, используемые подразделением или сотрудником без ведома группы информационных технологий или безопасности организации. *Источник*: Cisco www.cisco.com/c/en/us/products/security/what-is-shadow-it.html
Социальная инженерия	Манипулирование людьми с целью выполнения теми определенных действий или разглашения информации, полезной для злоумышленника. *Источник*: Национальный центр кибербезопасности (Соединенное Королевство) www.ncsc.gov.uk/information/ncsc-glossary
Целевой фишинг	Использование поддельных электронных писем для того, чтобы убедить сотрудников организации раскрыть свои имена пользователя или пароли. В отличие от фишинга, при котором используется массовая рассылка, целевой фишинг узко направлен на четко определенную цель. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary

Спуфинг	Подделка адреса отправителя передачи с целью незаконного проникновения в безопасную систему. *Источник*: Комитет по системам национальной безопасности (Соединенные Штаты) https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
Виртуальная частная сеть	Частная сеть связи, обычно используемая внутри компании или несколькими разными компаниями или организациями для связи по более широкой сети. В виртуальной частной сети сообщения обычно зашифрованы или инкапсулированы для защиты от перехвата другими пользователями в сети общего пользования, в которой построена виртуальная частная сеть. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary
Уязвимость	Изъян или слабое место в разработке или реализации информационной системы или ее среды, которые могут быть использованы для неблагоприятного воздействия на ресурсы или деятельность организации. *Источник*: Канадский центр кибербезопасности https://cyber.gc.ca/en/glossary

Приложение X

Сводка действий, которые должны быть предприняты участвующими организациями по рекомендациям Объединенной инспекционной группы

		Предполагаемое воздействие	*Организация Объединенных Наций*																												
			МВЦ	*Организация Объединенных Наций*	*ЮНЭЙДС*	*ЮНКТАД*	*МТЦ*	*ПРООН*	*ЮНЕП*	*ЮНФПА*	*Хабитат ООН*	*УВКБ*	*ЮНИСЕФ*	*УНП*	*ЮНОПС*	*БАПОР*	*ООН-женщины*	*ВПП*	*ФАО*	*МАГАТЭ*	*ИКАО*	*МОТ*	*ИМО*	*МСЭ*	*ЮНЕСКО*	*ЮНИДО*	*ЮНВТО*	*ВПС*	*ВОЗ*	*ВОИС*	*ВМО*
			Организация Объединенных Наций и ее фонды и программы																*Специализированные учреждения и МАГАТЭ*												
Доклад	Для принятия мер		☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	Для информации		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Рекомендация 1		**f**		**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**	**И**
Рекомендация 2		**f**		**Д**	**Д**			**Д**	**Д**	**Д**			**Д**		**Д**		**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**	**Д**
Рекомендация 3		**c**	**И**																												
Рекомендация 4		**c**		**Д**																											
Рекомендация 5		**f**		**И**																											

Условные обозначения:

Д: рекомендация для принятия решения директивным органом

И: рекомендация для принятия мер исполнительным главой

: рекомендация не требует принятия мер этой организацией

Предполагаемое воздействие: a: повышение прозрачности и ответственности; **b:** распространение полезного/передового опыта; **c:** усиление координации и сотрудничества; **d:** усиление согласованности и последовательности; **e:** усиление контроля и соблюдения правил; **f:** повышение эффективности; **g:** значительная финансовая экономия; **h:** повышение эффективности; **i:** прочее.