Организация Объединенных Наций A/68/552

Генеральная Ассамблея

Distr.: General
25 October 2013
Russian
Original: English

Шестьдесят восьмая сессия
Пункт 134 повестки дня
Предлагаемый бюджет по программам на двухгодичный период 2014–2015 годов

Деятельность по осуществлению рекомендаций, касающихся укрепления информационной и системной безопасности во всех подразделениях Секретариата

Доклад Генерального секретаря

Резюме

Настоящий доклад представляется в соответствии с пунктом 18 части I резолюции 67/254 Генеральной Ассамблеи, в котором Ассамблея просила Генерального секретаря представить в контексте предлагаемого бюджета по программам на двухгодичный период 2014–2015 годов обновленную информацию о ходе осуществления мер, принятых для решения задач по обеспечению защищенности информации. Проведенная независимая оценка и имевшие место в 2013 году случаи несанкционированного доступа к защищенной информации показали наличие существенных недостатков, которые создают неприемлемый уровень риска для Организации. В настоящем докладе излагаются меры, которые необходимо принять для противодействия любым угрозам кибератак, а также дополнительные потребности в ресурсах в размере 3 440 700 долл. США до пересчета по разделу 29E «Управление информационно-коммуникационных технологий» предлагаемого бюджета по программам на двухгодичный период 2014–2015 годов, необходимые для удовлетворения наиболее безотлагательных потребностей Организации в сфере обеспечения информационной безопасности.

13-53218 (R) 051113 061113

I. Введение

1. В пункте 107 резолюции 66/246 Генеральная Ассамблея просила Консультативный комитет по административным и бюджетным вопросам обратиться с просьбой к Комиссии ревизоров провести ревизию и оценку деятельности в области информационно-коммуникационных технологий (ИКТ) в Секретариате, в том числе деятельности Управления информационно-коммуникационных технологий, и представить Ассамблее в ходе основной части ее шестьдесят седьмой сессии доклад по этому вопросу. Комиссия провела эту ревизию в октябре 2012 года, а 19 декабря 2012 года представила свой доклад (A/67/651) Генеральному секретарю.

2. В пункте 95 своего доклада Комиссия ревизоров указала, что Организация Объединенных Наций не располагает надлежащей информационной защитой, а существующие системы обеспечения безопасности не соответствуют представлениям Комиссии о том, как этот вопрос должен решаться в современной глобальной организации. Она также указала, что Секретариат обладает крайне ограниченными возможностями для осуществления текущего контроля за угрозами несанкционированного доступа и, таким образом, не может надлежащим образом выявлять все удавшиеся или неудавшиеся попытки проникновения в защищенные системы и реагировать на них.

3. В одном из последующих докладов по вопросу о выполнении рекомендаций Комиссии ревизоров (A/67/651/Add.1) Генеральный секретарь указал, что рекомендации, касающейся укрепления информационной и системной безопасности во всех подразделениях Секретариата, уделяется самое первостепенное внимание и что администрация разрабатывает план действий, который будет включать краткосрочные меры, призванные устранить наиболее явные недостатки, и предусматривать разработку последовательной стратегии обеспечения информационной безопасности на среднесрочную и долгосрочную перспективу. Этот план действий включает 10 инициатив, в которых основное внимание уделяется следующим 3 областям:

a) меры превентивного контроля. Секретариат укрепит системы технического контроля в инфраструктуре ИКТ, призванные:

i) обеспечить более жесткий контроль за вычислительными устройствами, подключенными к сети Организации Объединенных Наций;

ii) воспрепятствовать доступу к вредоносному интернет-трафику и сообщениям электронной почты путем укрепления мер технической защиты периметра сети Организации Объединенных Наций;

iii) обеспечить сегментирование сети в целях изолирования тех ее участков, где вирусы могут маскировать угрозу атак;

iv) обеспечить путем обучения сотрудников Организации Объединенных Наций и проведения соответствующей разъяснительной работы среди них более широкое распространение информации по вопросам обеспечения безопасности;

b) более эффективная система обнаружения инцидентов и реагирования на них. В целях адаптации к условиям, характеризующимся существенным повышением степени риска, Секретариат внедрит дополнительные системы выявления попыток несанкционированного вторжения и обеспечит систематический контроль за работой своих сетей;

c) система управления, риски и соблюдение нормативов. Предполагается утвердить и реализовать на практике директиву по вопросам обеспечения информационной безопасности, в которой будут определены основополагающие принципы информационной защиты в Организации Объединенных Наций и которая станет основой для разработки соответствующих стратегий и нормативных документов.

4. Впоследствии Консультативный комитет по административным и бюджетным вопросам в своих комментариях по докладу Комиссии ревизоров о решении вопросов, связанных с информационно-коммуникационными технологиями в Секретариате (A/67/770), рекомендовал просить Генерального секретаря при подготовке его предложений по осуществлению плана действий в сфере обеспечения информационной безопасности приложить все усилия к тому, чтобы определить приоритетные цели и соответственно перераспределить ресурсы во избежание, насколько это возможно, представления запросов на выделение дополнительных ресурсов. Кроме того, Консультативный комитет указал, что он разделяет опасения Комиссии по поводу ситуации в сфере информационной безопасности. Он рекомендовал просить Генерального секретаря незамедлительно приступить к осуществлению его плана действий и обеспечить принятие без дальнейшего промедления хартии информационной безопасности и соответствующих директивных документов таким образом, чтобы добиться подотчетности во всех подразделениях Секретариата. Помимо этого, Консультативный комитет указал, что Генеральному секретарю следует в срочном порядке принять меры для устранения любых препятствий, которые могли бы помешать эффективному осуществлению плана действий или утверждению и внедрению в Секретариате стратегий в сфере информационной безопасности, а также рекомендовал просить Генерального секретаря представить в контексте предлагаемого бюджета по программам на двухгодичный период 2014–2015 годов обновленную информацию о ходе выполнения мер, принятых для решения задач в сфере обеспечения информационной безопасности. Комитет далее просил Комиссию ревизоров проконтролировать выполнение его рекомендаций в этой области.

5. После этого Генеральная Ассамблея в пункте 11 части I своей резолюции 67/254 просила Генерального секретаря представить доклад о ходе осуществления мер, принятых для решения первоочередных задач, определенных Комиссией в ее докладе (A/67/651), в том числе в связи с обеспечением защиты информационно-технических систем, а в пункте 18 просила Генерального секретаря представить в контексте предлагаемого бюджета по программам на двухгодичный период 2014–2015 годов обновленную информацию о ходе осуществления мер, принятых для решения задач по обеспечению защищенности информации, включая меры, принятые для противодействия любым угрозам кибератаки.

II. Ситуация в настоящее время

6. Генеральный секретарь активно занимается вопросами осуществления плана действий по укреплению информационной безопасности во всех подразделениях Секретариата и уделяет основное внимание наиболее важным и требующим принятия безотлагательных мер аспектам этого плана действий в Центральных учреждениях. На сегодняшний день Управление информационно-коммуникационных технологий прилагает все усилия для пересмотра приоритетности целей и соответствующего перераспределения ресурсов в рамках утвержденных ассигнований и для покрытия, в пределах возможного, расходов на проведение практических мероприятий в поддержку инициатив, предусмотренных в плане действий. Вместе с тем этих ресурсов явно недостаточно для того, чтобы надлежащим образом устранить все выявленные недостатки. Кроме того, со времени публикации доклада Комиссии ревизоров во всем мире было отмечено значительное увеличение числа и повышение уровня сложности нападений на защищенные информационные системы, с некоторыми из которых непосредственно столкнулся Секретариат.

7. Учитывая эти инциденты, Генеральный секретарь считает необходимым принять безотлагательные меры в дополнение к тому, что уже сделало Управление информационно-коммуникационных технологий.

III. Первоначальные меры на пути осуществления плана действий по укреплению информационной безопасности

8. Планом действий предусматривается устранение в порядке первоочередности наиболее явных недостатков в сфере обеспечения информационной безопасности, а также разработка последовательной стратегии среднесрочных и долгосрочных действий по укреплению информационной безопасности в Секретариате. С учетом нехватки квалифицированных специалистов в Секретариате и необходимости проведения исчерпывающего анализа существующей в Организации политики в сфере обеспечения безопасности было принято решение о необходимости привлечения внешних специалистов для оценки и/или проверки потенциального риска. В июле 2013 года Управление информационно-коммуникационных технологий постановило провести независимую оценку положения в сфере обеспечения информационной безопасности в Секретариате и привлечь для этой цели внешнюю консультационную фирму, которая бы проверила и дополнила выводы, сделанные по итогам внутренней проверки, и определила уязвимые места и оперативные недостатки Организации в сфере информационной защиты. Эта независимая оценка, а также новые случаи несанкционированного доступа к защищенным данным, имевшие место в 2013 году, показали наличие существенных недостатков, вследствие которых Организация подвергается неприемлемым рискам.

9. В 2014 году с учетом выводов независимой оценки, в ходе которой основное внимание уделялось инфраструктуре в Нью-Йорке, Генеральный секретарь пришел к выводу о необходимости дальнейшего укрепления информационной безопасности в Центральных учреждениях, безотлагательного проведения более широкой независимой оценки в контексте увеличения числа кибератак на Организацию, а также о необходимости расширения сферы охвата мероприя-

тий по дальнейшему укреплению информационной безопасности отделений за пределами Центральных учреждений, региональных комиссий и полевых миссий. Информация, полученная в рамках взаимодействия с этими отделениями, свидетельствует о том, что предстоит многое сделать для устранения существующих в них недостатков. Кроме того, хотя отделения на местах, пользующиеся услугами Департамента полевой поддержки, могут быть менее уязвимыми, поскольку соответствующие услуги централизованно обеспечиваются Вспомогательной базой Организации Объединенных Наций в Валенсии, Испания, и Базой материально-технического снабжения Организации Объединенных Наций в Бриндизи, Италия, существующие в этих отделениях недостатки также необходимо подвергнуть тщательному анализу.

10. Ниже приводится детальная информация о мерах, которые уже были приняты для осуществления плана действий:

a) были ужесточены меры превентивного контроля путем ограничения административных прав на новых или прошедших модернизацию стационарных или портативных компьютерах, которые выдаются сотрудникам в пользование. В настоящее время осуществляется закупка дополнительных систем фильтрации сообщений электронной почты и интернет-трафика, которая должна завершиться к концу ноября 2013 года. Кроме того, осуществляется перенастройка серверов, на которые устанавливаются обновленные системы защиты, отвечающие самым современным требованиям, в целях устранения потенциальных уязвимостей в их защите. Были проанализированы параметры инфраструктуры брандмауэр-систем в Центральных учреждениях и принято решение заменить их более современными техническими средствами, которые позволяют обеспечить более высокий уровень защиты от внешних атак и предусматривают внутреннее сегментирование сети. Кроме того, было закуплено обучающее программное обеспечение в целях повышения осведомленности всех сотрудников Секретариата о вопросах информационной безопасности;

b) начато проведение анализа всех пакетов программного обеспечения, используемых в настоящее время, на предмет проверки их соответствия стандартам и передовой практике в сфере обеспечения защиты информации. Это мероприятие проводится в рамках выявления всех пакетов программного обеспечения, которые будут сохранены после внедрения системы «Умоджа» и других общеорганизационных систем, а также в целях обеспечения того, чтобы они не создавали угрозу безопасности;

c) в основных центрах хранения и обработки данных, т.е. в первичном и вторичном центрах, расположенных в Нью-Йорке и Нью-Джерси, а также в центрах хранения и обработки общеорганизационной информации на Вспомогательной базе и Базе материально-технического снабжения налажено дистанционное управление услугами по развертыванию и текущему обслуживанию систем выявления попыток несанкционированного доступа. Кроме того, были сведены воедино действующие в различных подразделениях Секретариата центры анализа киберугроз в целях укрепления их потенциала по заблаговременному корректированию мер защиты;

d) 7 марта 2013 года была разработана и доведена до сведения руководителей всех департаментов и подразделений директива с изложением политики в сфере обеспечения информационной безопасности, которая является общей рамочной основой политики, процедур и руководящих принципов Органи-

зации в сфере защиты информации. Кроме того, этой директивой предусматривается необходимость регистрации попыток доступа к защищенной информации и необходимость распространения среди всех подразделений Секретариата аналитической информации, на основе которой можно было бы принимать конкретные меры. На базе проекта, подготовленного Управлением информационно-коммуникационных технологий, Специальная группа по вопросам информационной безопасности Координационного совета руководителей системы Организации Объединенных Наций (КСР) подготовила свод технических и процедурных нормативов, предусматривающих минимальные требования к открытым веб-сайтам, которые были одобрены сетью ИКТ в рамках Комитета высокого уровня по вопросам управления КСР. Кроме того, в настоящее время разрабатываются 52 стратегии и процедуры по вопросам ИКТ, призванные способствовать повышению эффективности, надежности и отказоустойчивости систем. В 2014 году в сотрудничестве с Департаментом общественной информации этот документ будет опубликован в качестве административной инструкции, в которой будут рассматриваться вопросы снижения высокой уязвимости открытых веб-сайтов и предпринят анализ ряда случаев несанкционированного доступа к защищенной информации. Помимо этого, Управление информационно-коммуникационных технологий перераспределило ресурсы в целях налаживания внутреннего контроля за соблюдением принятых в Организации стратегий и процедур и обеспечения соответствия передовой практике в этой сфере. Управление также учредило рабочую группу по вопросам информационной безопасности в рамках Координационной группы по вопросам управления ИКТ в целях расширения взаимодействия между местами службы, включая отделения за пределами Центральных учреждений, региональные комиссии и полевые миссии.

11. В дополнение к мерам, принимаемым в рамках плана действий, Организация вносит существенные изменения в практику использования ИКТ в масштабах всей Организации, с учетом и в поддержку внедрения системы «Умоджа» и других вспомогательных систем. Эти изменения включают, в частности, создание новой общесекретариатской распределенной сети на базе многопротокольной маркёрной коммутации, стандартизацию уровней доступа с помощью системы Citrix для всех общеорганизационных систем, а также перевод программных комплексов в общеорганизационные центры хранения и обработки данных в Валенсии и Бриндизи. Эти изменения позволят ужесточить контроль за доступом и обеспечить более четкое управление инфраструктурой ИКТ, а также снизить ее уязвимость к попыткам несанкционированного доступа.

12. Кроме того, защита ИКТ в качестве одного из важнейших элементов обеспечения бесперебойного функционирования и послеаварийного восстановления систем имеет большое значение для полевых миссий с учетом условий, в которых они работают. Недавно Департамент полевой поддержки разработал рамочную политику в сфере обеспечения защиты, в которой основной упор делается на созданный в Департаменте Центр оперативно-технической поддержки на местах, который задействуют ИКТ-объекты на Вспомогательной базе и Базе материально-технического снабжения. В соответствии с этим рамочным директивным документом в Центре оперативно-технической поддержки на местах и полевых миссиях проводятся регулярные проверки информаци-

онных систем, инфраструктуры и других информационных ресурсов на предмет определения их защищенности.

IV. Необходимые дополнительные меры

13. По итогам проведенной независимой оценки и с учетом имевших место в 2013 году случаев несанкционированного доступа к защищенной информации стало очевидно, что существующие в Организации Объединенных Наций механизмы защиты информации не отвечают предъявляемым требованиям, причем речь идет не только о традиционных элементах инфраструктуры ИКТ, но и о других элементах инфраструктуры. Системы эксплуатации зданий, контролирования и ограничения доступа, организации телефонной и видеосвязи, а также аудиовизуальные средства, которые традиционно обходились без цифрового контроля, теперь также стали уязвимыми перед лицом цифровых угроз, а возможно и угроз, проистекающих из интернета. Потребуется провести дополнительный подробный анализ на предмет учета этих устройств во всеобъемлющей стратегии в сфере информационной безопасности.

14. Проведенный анализ систем, используемых в Департаменте полевой поддержки, продемонстрировал необходимость внедрения новых программных средств для отслеживания попыток несанкционированного доступа и фильтрации трафика, а также обновленных брандмауэр-систем в целях укрепления защиты информации в Организации как в указанных точках, так и в других местах службы. Уже приняты новые меры для обеспечения информационной защиты и ведется дополнительная работа в этом направлении.

15. Кроме того, было установлено, что оперативные недостатки в сфере управления веб-информацией могут создать дополнительную угрозу для репутации Организации. В соответствии с этим Организация пришла к выводу о необходимости проведения тщательного анализа веб-сайтов, размещенных на внешних серверах, пересмотра механизмов контроля и оказания помощи департаментам Секретариата в сфере переработки веб-сайтов в целях укрепления их защиты от несанкционированных вторжений или искажения их внешнего вида.

16. Всеобъемлющая стратегия обеспечения информационной безопасности, охватывающая системы, основанные на веб-технологиях, и нетрадиционные системы, а также исходные системные проблемы, станет центральной частью общей стратегии в сфере ИКТ, которая будет представлена на рассмотрение Генеральной Ассамблеи на ее шестьдесят девятой сессии.

17. Тем временем необходимо срочно принять дополнительные меры для дальнейшего снижения уровня неприемлемых рисков для Организации на основе уже достигнутого прогресса путем осуществления плана действий по укреплению информационной безопасности во всех подразделениях Секретариата.

18. В связи с увеличением потребностей в межсетевом взаимодействии и взаимозависимости ИКТ-систем Секретариата нападение или вторжение на любом участке сети может нанести ущерб безопасности всех ее сегментов. Таким образом, необходимо, чтобы уже принятые меры по осуществлению плана действий распространялись и на другие места службы и подкреплялись значи-

тельным расширением потенциала Организации по осуществлению текущего контроля.

19. В качестве временных мер на период, пока не будет представлена пересмотренная стратегия в сфере ИКТ[1], предлагается принять следующие меры, для которых испрашиваются ресурсы в настоящем докладе:

a) распространение действия системы отслеживания попыток несанкционированного доступа на подразделения за пределами Центральных учреждений и региональные комиссии. За счет перераспределения ресурсов Управления информационно-коммуникационных технологий в 2013 году эта система уже внедрена и действует в основном и вспомогательном центрах хранения и обработки данных в Нью-Йорке и Нью-Джерси и общеорганизационных центрах хранения и обработки данных на Вспомогательной базе и Базе материально-технического снабжения. Вместе с тем в 2014 году потребуются дополнительные ресурсы для дальнейшего покрытия расходов на оказание услуг в уже охваченных этой системой местах службы и ее распространения на зарубежные места службы;

b) расширение охвата и модернизация инфраструктуры системы брандмауэр, а также обновление систем фильтрации сообщений электронной почты и интернет-трафика и подключение к ним отделений за пределами Центральных учреждений и региональных комиссий в целях укрепления механизмов обеспечения безопасности общеорганизационной сети;

c) укрепление внутреннего потенциала для осуществления текущего контроля за угрозами несанкционированного доступа к защищенным данным. Необходимы дополнительные технические средства и кадровые ресурсы в целях существенного расширения потенциала по осуществлению текущего контроля за ИКТ-средой на предмет отслеживания удачных или неудачных попыток несанкционированного доступа;

d) развертывание системы оценки степени защищенности и устранения недостатков, которые позволят Организации заблаговременно принимать меры для выявления конкретных проблем и направлять все усилия на их решение;

e) проведение дополнительных оценок механизмов защиты и отслеживания попыток несанкционированного доступа к нетрадиционным элементам инфраструктуры в Центральных учреждениях и ИКТ-сетям отделений за пределами Центральных учреждений, региональных комиссий и общеорганизационных центров хранения и обработки данных в Валенсии и Бриндизи.

20. Ясно, что разобщенность ИКТ-сетей Организации затрудняет обеспечение их защиты и делает эту задачу более дорогостоящей. Принятая в Организации стратегия заключается в том, чтобы оперативно перевести ее центры хранения и обработки данных в Валенсию и Бриндизи в интересах обеспечения возможности ускоренного развертывания системы обеспечения безопасности и контроля при одновременном повышении оперативности систем и снижении расходов. Кроме того, ликвидация такой разобщенности является одним из основных элементов новой стратегии в сфере ИКТ, которую Генеральный

[1] С учетом того, что эти меры носят секретный характер и в целях сведения к минимуму оперативных рисков, в настоящем докладе приводится лишь общее описание.

секретарь предложит для рассмотрения Генеральной Ассамблеи на ее шестьдесят девятой сессии.

V. Необходимые изменения программы работы на период 2014–2015 годов

21. Чтобы надлежащим образом решить вопросы обеспечения информационной безопасности в Секретариате, потребуется пересмотреть утвержденную программу работы Управления информационно-коммуникационных технологий на период 2014–2015 годов (A/67/6/Rev.1, prog. 25) и включить в нее мероприятия по осуществлению подпрограммы 5 «Стратегическое управление и координация в сфере применения информационно-коммуникационных технологий».

VI. Дополнительные потребности по предлагаемому бюджету по программам на двухгодичный период 2014–2015 годов

22. Дополнительные потребности в ресурсах, сформулированные в настоящем докладе, основываются на результатах независимой оценки, проведенной в 2013 году после представления Генеральным секретарем предлагаемого бюджета по программам на двухгодичный период 2014–2015 годов (A/68/6 (Sect. 29E)), и вызваны увеличением числа и частоты кибератак на Организацию Объединенных Наций. Этим объясняются испрашиваемые дополнительные ассигнования на осуществление мероприятий, подробно описываемых ниже.

23. Как видно из таблицы 1 ниже, сметные расходы в общем объеме 3 440 700 долл. США до пересчета потребуются на 12-месячный период по разделу 29E в целях устранения наиболее явных проблем Организации в сфере обеспечения информационной безопасности, которые подробно описаны в настоящем докладе, до рассмотрения Генеральной Ассамблеей на ее шестьдесят девятой сессии пересмотренной стратегии в сфере ИКТ.

Таблица 1
Сводные потребности с разбивкой по статьям расходов
(В тыс. долл. США)

Статья расходов	*Смета на 2014–2015 годы*
Прочие расходы по персоналу	581,4
Поездки персонала	150,0
Услуги по контрактам	1 325,0
Общие оперативные расходы	59,3
Мебель и оборудование	1 325,0
Всего	**3 440,7**

Таблица 2
Потребности в ресурсах по разделу 29E предлагаемого бюджета по программам на двухгодичный период 2014–2015 годов до пересчета
(В тыс. долл. США)

Статья расходов	*Ассигнования (A/68/6 (Sect. 29E))*	*Дополнительные потребности*	*Общие потребности*
Должности	36 168,6	–	36 168,6
Прочие расходы по персоналу	5 634,0	581,4	6 215,4
Поездки персонала	467,8	150,0	617,8
Услуги по контрактам	12 697,0	1 325,0	14 022,0
Общие оперативные расходы	16 574,5	59,3	16 633,8
Принадлежности и материалы	202,4	–	202,4
Мебель и оборудование	948,2	1 325,0	2 273,2
Всего	**72 692,5**	**3 440,7**	**76 133,2**

Прочие расходы по персоналу

24. Ассигнования в размере 581 400 долл. США предназначены для покрытия расходов на оплату услуг временного персонала общего назначения в течение 12-месячного периода для выполнения функций, связанных с устранением наиболее явных недостатков в сфере обеспечения защиты в рамках пересмотра и внедрения принятой Управлением по информационно-коммуникационным технологиям практики в сфере обеспечения защиты и соответствующих мер реагирования на попытки несанкционированного доступа. Требуется учредить следующие временные должности:

a) одну должность временного сотрудника категории общего обслуживания, эквивалентную уровню С-4, который будет выполнять функции инженера по системам безопасности. Этот сотрудник будет выполнять дополнительные технические функции, связанные с эксплуатацией недавно внедренной системы выявления попыток несанкционированного доступа. Предполагается, что в месяц Организация будет сталкиваться как минимум с 70 000–100 000 покушений на ее системы защиты. Этот инженер по системам безопасности будет сотрудничать с внешним подрядчиком в целях систематического отслеживания требующих принятия безотлагательных мер попыток несанкционированного доступа и заниматься принятием соответствующих мер. По мере развертывания системы отслеживания попыток несанкционированного доступа в отделениях за пределами Центральных учреждений и региональных комиссиях он будет заниматься сбором соответствующей информации по всей Организации. Необходимо обеспечить координацию деятельности по комплексному отслеживанию таких попыток и принятию соответствующих мер противодействия на уровне всей Организации. Такая координация будет иметь важнейшее значение для обеспечения эффективности более широкого анализа функционирования сети, обеспечиваемого системой отслеживания попыток несанкционированного доступа. Кроме того, инженер по системам безопасности может оказывать помощь в процессе анализа и обеспечения функционирования системы брандмауэр следующего уровня;

b) две должности временных сотрудников общего назначения, эквивалентных должностям уровня С-3, для выполнения новых функций, связанных с анализом вредоносных программных средств, анализа характера действия вредоносного программного обеспечения и сопоставления информации об атаках, что имеет важнейшее значение для определения того, каким атакам Организация может подвергаться в результате постоянной угрозы повышенной сложности, происходящей из различных источников по всему миру. Кроме того, этот сотрудник будет заниматься укреплением существующего потенциала тестирования возможностей несанкционированного доступа, анализом слабых мест, представлять сообщения о тестировании систем защиты веб-приложений и координировать работу в этой сфере. Этот сотрудник может также поддерживать контакты с группами специалистов по разработке программного обеспечения в целях ужесточения стандартов создания защищенного программного обеспечения и их тестирования во всех подразделениях Организации.

Поездки персонала

25. Ассигнования в размере 150 000 долл. США испрашиваются для покрытия расходов на поездки двух сотрудников во все отделения за пределами Центральных учреждений, региональные комиссии и центры хранения и обработки данных Организации в Валенсии и Бриндизи продолжительностью минимум в две недели в целях:

a) безотлагательного проведения независимых проверок соблюдения мер безопасности и проведения технических тестов, необходимых для обеспечения соблюдения и регулярной проверки соблюдения существующих политики и стандартных оперативных процедур. Эта деятельность предусматривает оценку, проверку и документирование местных проблем, которые ранее не регистрировались, и угроз информационной безопасности. Кроме того, она позволит сотрудникам Центральных учреждений осуществлять контроль за их соблюдением и сообщать о недостатках, что имеет важнейшее значение для осуществления центральной стратегии обеспечения безопасности ИКТ;

b) оказания технической консультативной и иной поддержки в осуществлении политики, а также проведения проверки всех новых систем и приложений, которые планируется внедрить;

c) проведения совещаний, а также практических занятий на местах для всех пользователей и технических специалистов, чтобы обеспечить понимание и эффективное внедрение во всех местах службы проектно-архитектурных решений превентивных мер по защите информации.

26. Испрашиваемые ресурсы по этой категории предназначены для покрытия расходов на поездки сотрудников в тех случаях, когда проведение онлайновой и/или аудиоконференции представляется нецелесообразным вследствие конфиденциального характера соответствующей работы. В пределах возможного будет сохраняться практика совмещения командировок в целях обеспечения более эффективного использования ресурсов.

Услуги по контрактам

27. Ассигнования в размере 1 325 000 долл. США испрашиваются для покрытия следующих потребностей:

a) услуги по выявлению попыток несанкционированного доступа (800 000 долл. США) в рамках развертывания и текущего обслуживания соответствующих систем, которые внедряются в процессе осуществления плана действий. Первые компоненты этой системы в Нью-Йорке, Бриндизи и Валенсии были установлены за счет перераспределения имеющихся ресурсов. Вместе с тем в целях охвата этой системой всех подразделений Секретариата необходимо наладить такие услуги во всех центрах хранения и обработки данных и всех местах службы. Возможность отслеживать попытки несанкционированного доступа имеет важнейшее значение для того, чтобы Организация могла своевременно реагировать на них;

b) система выявления недостатков в защите (25 000 долл. США), которая будет систематически и периодически анализировать все используемые в Организации Объединенных Наций средства ИКТ, такие как серверы и другие важнейшие системы, чтобы обеспечивать их правильную конфигурацию и своевременную установку важнейших обновлений программного обеспечения защиты, упрощать управление такими активами и выявлять недостатки в системах защиты, прежде чем ими смогут воспользоваться злоумышленники;

c) индивидуальное обслуживание (500 000 долл. США) высококвалифицированных специалистов в процессе проведения ими необходимых мероприятий, имеющих важнейшее значение для осуществления стратегии обеспечения информационной защиты в Секретариате, включая внедрение новых технических средств и проведение дополнительной оценки важнейших элементов инфраструктуры. Кроме того, возникнет краткосрочная потребность в услугах высококвалифицированных специалистов для решения конкретных технических проблем и оказания дополнительной помощи в сфере проведения экспертизы или расследований, которые позволят получить самое полное представление о процедурах решения проблем в сфере обеспечения информационной безопасности. Работая по краткосрочным контрактам, такие специалисты будут выполнять узкоспециальные функции и передавать полученные знания штатным сотрудникам.

Общие оперативные расходы

28. Ассигнования в размере 59 300 долл. США предназначены для покрытия расходов на аренду служебных помещений (47 700 долл. США) и связаны с соглашением об уровне обслуживания (“A”) (6300 долл. США) для трех временных должностей в Нью-Йорке, а также для покрытия расходов на локальную вычислительную сеть (1800 долл. США) и оплаты услуг связи (3500 долл. США).

Мебель и оборудование

29. Ассигнования в размере 1 325 000 долл. США предназначены для удовлетворения следующих потребностей:

a) системы постоянного слежения (200 000 долл. США). Централизованный сбор и анализ системных журналов дополняет данные системы отслеживания попыток несанкционированного доступа и дает Организации возможность выявлять нештатные или подозрительные операции, которые нельзя считать злонамеренными. Такая система не только позволяет выявлять нарушения и малозаметные попытки несанкционированного доступа, но и дает возможность анализировать главные причины, по которым такие нарушения стали возможны, после обнаружения этих нарушений и определения их масштабов. Система управления информацией и выдачи оповещений о попытках несанкционированного доступа, которую предлагается закупить, включает специальные аппаратно-программные средства и лицензии, стоимость которых устанавливается с учетом объема поступающей информации;

b) укрепление инфраструктуры брандмауэра (1 млн. долл. США), включая модернизацию существующих брандмауэров (500 000 долл. США) и систем фильтрации (500 000 долл. США) с помощью самых современных брандмауэров и систем фильтрации содержания следующего поколения, которые позволят Организации пресекать или выявлять попытки атак и вторжений, совершаемых таким образом, чтобы их нельзя было засечь традиционными средствами. Это обновление имеет важнейшее значение в условиях постоянно меняющегося характера атак, которым подвергается Организация. Работа в этом направлении уже началась в Центральных учреждениях и общеорганизационных центрах хранения и обработки данных в Валенсии и Бриндизи за счет перераспределения существующих ресурсов, выделенных в 2013 году. Вместе с тем эту деятельность необходимо распространить на все центры хранения и обработки данных и места службы;

c) тестирование защиты веб-приложений (125 000 долл. США), включая закупку более современных средств тестирования защиты веб-приложений в форме лицензий на программное обеспечение как услугу для использования на местах или третьими сторонами в масштабах всей Организации. Эти средства могут использоваться собственными сотрудниками по вопросам обеспечения защиты и/или разработчиками веб-приложений в целях укрепления защиты веб-сайтов Организации Объединенных Наций.

VII. Решения, которые предлагается принять Генеральной Ассамблее

30. **Генеральной Ассамблее предлагается:**

a) принять настоящий доклад к сведению;

b) утвердить дополнительные ассигнования в размере 3 440 700 долл. США по разделу 29E «Управление информационно-коммуникационных технологий» предлагаемого бюджета по программам на двухгодичный период 2014–2015 годов в целях удовлетворения безотлагательных потребностей по укреплению защиты систем ИКТ в Секретариате. Эта сумма подлежит покрытию за счет средств резервного фонда.