Всемирная организация здравоохранения

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ
148-я сессия **EB148/30**
Пункт 18.1 предварительной повестки дня **11 января 2021 г.**

Обновленная информация по управлению информацией и информационным технологиям

Доклад Генерального директора

1. В январе 2020 г. на тридцать первом заседании Комитета Исполкома по программным, бюджетным и административным вопросам Секретариат представил доклад, в котором сообщил о своих инициативах в области кибербезопасности[1]. Кроме того, в последнем отчете внутреннего ревизора[2], рассмотренном на тридцать втором заседании Комитета, особое внимание было уделено ключевым элементам ревизии дорожной карты по обеспечению кибербезопасности. Настоящий доклад представлен в ответ на поручение Комитета Секретариату представить доклад об управлении в области кибербезопасности.

ПРОГРЕСС, ДОСТИГНУТЫЙ ДО ПАНДЕМИИ

2. Кибербезопасность является одной из областей, в которых должны быть достигнуты ключевые результаты в рамках стратегии по управлению информацией и информационным технологиям. Цель заключается в том, чтобы защитить цифровые ресурсы Секретариата, повысить безопасность данных и обеспечить возможность предоставления услуг с приемлемым уровнем риска.

3. Инициативы, предпринятые в поддержку обеспечения кибербезопасности, в том числе включали проведение обязательного для всех сотрудников Организации обучения в целях повышения информированности в вопросах кибербезопасности; проведение ежемесячных регулярных учений по борьбе с фишингом; проведение ежегодного мероприятия по повышению информированности по вопросам кибербезопасности; создание центрального хранилища системных журналов для целей судебной экспертизы; стандартизация управления межсетевой зашитой; внедрение глобальной системы защиты от вирусов; ведение в действие системы фильтрации сетевого трафика в Интернете и внедрение сбора информации о киберугрозах, которая позволяет принимать упреждающие меры во избежание будущих и прогнозируемых инцидентов.

4. Секретариат также создал специальную независимую группу по кибербезопасности. Кроме того, он приступил к созданию целевого комплексного оперативного центра по обеспечению безопасности, обеспечивающего идентификацию,

[1] Документ EB146/40.

[2] Документ A73/28.

предотвращение и выявление кибератак, а также защиту от них и реагирование на них в случае их возникновения.

5. Повышение эффективности деятельности в области управления было обеспечено путем: публикации принятой стратегии по кибербезопасности, создания дорожной карты по обеспечению кибербезопасности и разработки глобальной политики, правил, стандартов и стандартных операционных процедур; создания Совета по кибербезопасности; и пересмотра устава глобального руководящего комитета по вопросам информационных технологий в ответ на необходимость обеспечения всеобъемлющей ответственности за кибербезопасность.

МЕРЫ РЕАГИРОВАНИЯ НА СВЯЗАННЫЕ С ПАНДЕМИЕЙ COVID-19 КИБЕРАТАКИ

6. После объявления пандемии COVID-19 Секретариат отметил увеличение числа целенаправленных кибератак. К ним относятся выборочный фишинг, имперсонация, фишинг, вишинг (голосовой фишинг) и атаки на ИТ-инфраструктуру и приложения. В период с марта по май 2020 г. было зарегистрировано более 130 000 доменов по тематике COVID-19, из которых 70% были оценены исследователями как поддельные и использовались для многочисленных кибератак.

7. Продолжается значительное увеличение количества и сложности кибератак. Первоначальное решение по сбору информации о киберугрозах было сочтено недостаточным. Седьмого мая 2020 г. было внедрено новое решение по выявлению дополнительных угроз со стороны групп, создающих постоянные киберугрозы с применением новейших технологий. Это позволило Секретариату действовать более оперативно при восстановлении функций существующих ИТ-инфраструктуры, систем и инструментов.

8. Однако, как показал анализ тенденций, проведенный компаниями, специализирующимися в области кибербезопасности, кибератаки, по всей видимости, будут продолжаться. Необходимо постоянно активизировать усилия по выявлению и предотвращению кибератак, а также по защите от них, их обнаружению, реагированию на них и восстановлению после них. В связи с этим Секретариат активизировал работу по осуществлению программы кибербезопасности. **К числу принятых ключевых мер,** в том числе относятся те, которые указаны ниже.

(a) **Финансирование.** В отчете внутреннего ревизора за октябрь 2020 г.[1] отмечается, что полученных 1,3 млн долл. США недостаточно для реализации дорожной карты по обеспечению кибербезопасности. Глобальный руководящий комитет по вопросам информационных технологий предоставил дополнительно 4,7 млн долл. США, выделив в общей сложности 6 млн долл. США на эту программу.

(b) **Группа по кибербезопасности.** Численный состав этой группы был увеличен с шести до 11 человек, при этом соответствующие кадровые ресурсы находились в

[1] Документ A73/28.

Женеве и Будапеште. Была создана «красная группа» для проведения наступательных действий по проверке безопасности ИТ-систем, включая выявление уязвимости систем и оценку рисков.

(c) **Создание автоматизированного центра комплексного мониторинга информационной безопасности.** В июне 2020 г. был создан автоматизированный центр мониторинга информационной безопасности, в рамках которого мониторинг информационной безопасности интегрирован в деятельность по информированию в области безопасности и управлению событиями. Этот центр позволяет получать информацию о всех инцидентах, связанных с безопасностью, и помогает Секретариату уделять первоочередное внимание резкому увеличению числа событий в области. В период с августа по ноябрь 2020 г. было выявлено 14,5 миллиарда инцидентов в области безопасности. Благодаря работе центра мониторинга информационной безопасности Секретариат смог обеспечить проведение соответствующей фильтрации, обработки и анализа информации в связи с 243 серьезными инцидентами, связанными с нарушением безопасности, и сосредоточить свои усилия на их урегулировании.

(d) **Более эффективное обеспечение аутентификации пользователей.** Секретариат дополняет традиционные методы аутентификации (такие, как имя пользователя и аутентификация паролей) функциями по многофакторной аутентификации (например, используя программные токены) для подтверждения личности пользователя. Завершена работа по полному внедрению многофакторной аутентификации, которая используется при оказании Секретариатом всех услуг через Интернет.

(e) **Непрерывный мониторинг ИТ-ресурсов Организации.** В ответ на потребность в постоянном мониторинге и реагировании на угрозы в отношении ИТ-ресурсов Организации Секретариат внедрил систему обнаружения угроз и реагирования на конечных точках с использованием инструментов, предназначенных для обнаружения, сдерживания (при необходимости) и расследования подозрительных действий. Она позволяет получать информацию в рамках всей рабочей среды и создает возможности для своевременного обнаружения, защиты и реагирования. На сегодняшний день система охватывает 88% всех компьютеров и серверов во всех подразделениях Организации, и ведется работа по завершению 100% внедрения системы ко второму кварталу 2021 г.

(f) **Система предотвращения имперсонации в случае публичной рассылки сообщений по электронной почте от имени Организации.** С почтовых адресов с доменным именем <-who.int> в среднем ежемесячно отправляется 2,3 миллиона уникальных электронных сообщений. В апреле 2020 г. около 80% таких сообщений были отправлены с использованием имперсонации. В мае 2020 г. в целях минимизации последствий таких действий и предоставления возможностей для отправки сообщений от имени Организации только уполномоченным лицам Секретариат внедрил систему аутентификации сообщений, отчетности и обеспечения соответствия требованиям с использованием технологии доменов (DMARC). После этого 96% всех электронных сообщений полностью соответствовали предъявляемым требованиям, а остальные 4%, отправленные с

использованием имперсонации, были удалены и не попали в почтовые ящики организаций, которые внедрили систему DMARC.

(g) **Удаление устаревших приложений.** Старые системы, действующие на основе устаревших технологий, уязвимы для кибератак с применением новейших технологий. В настоящее время устанавливаются программные обновления для системы безопасности, однако в некоторых случаях устаревший дизайн и архитектура системы приводят к тому, что для обеспечения защиты от вредоносных атак таких обновлений становится недостаточно. По этой причине Секретариат заменил значительное число приложений, которые больше не поддаются восстановлению и исправлению.

9. Для эффективного управления программой кибербезопасности требуется осуществление постоянной коммуникации и координации. В частности:

(a) внутри Организации глобальная координация осуществляется отделом по кибербезопасности, в состав которого входят группа по кибербезопасности и представители всех регионов. Этот отдел координирует деятельность ВОЗ по обеспечению кибербезопасности, включая внедрение процедур, стандартов и решений в области кибербезопасности;

(b) в целях получения информации о киберугрозах и обмена такой информацией создан прямой канал связи с многочисленными компьютерными группами экстренного реагирования, правительственными организациями и частными компаниями. На ежедневной основе осуществляется обмен индикаторами компрометации.

10. Кроме того, осуществляется постоянный мониторинг работы корпоративных систем и приложений, включая Глобальную систему управления, электронную почту, веб-сайты, платформы по сотрудничеству и платформы разработок, и в целях уменьшения и устранения рисков в области кибербезопасности безотлагательно устанавливаются обновления для системы безопасности.

АКТИВИЗАЦИЯ УСИЛИЙ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

11. Нарушения в области кибербезопасности и результативные кибератаки обходятся весьма дорого. Потенциальные расходы включают затраты на возмещение материального и репутационного ущерба, понесенного Секретариатом; прямых финансовых потерь (в связи с восстановительными работами, потраченным рабочим временем, судебными издержками, расходами на деятельность по связям с общественностью и отправление уведомлений); а также издержек в связи с нарушением бесперебойной работы системы; потерей критически важных данных и целостности соответствующих данных.

12. Несмотря на все вышеупомянутые усилия, предпринятые Секретариатом, по-прежнему сохраняются проблемы, требующие решения, и имеется целый ряд областей, в которых необходимы улучшения. Важное значение для защиты Секретариата от структур, создающих постоянные угрозы с применением новейших технологий,

имеют следующие восемь новых направлений работы, которые включены в сферу охвата программы кибербезопасности.

(a) **Улучшенная защита электронной почты, с безопасными ссылками и вложениями.** Более 90% кибератак начинаются с фишинга через электронную почту с использованием ссылок и вложений. Встроенные функции безопасности электронной почты обеспечат защиту благодаря расширенной автоматической проверке вложений в электронные сообщения на вредоносный контент, и будет контролироваться время, затраченное на переход по ссылкам в сообщениях электронной почты.

(b) **Более безопасный доступ в Интернет.** Использование глобального облачного прокси-сервера обеспечит защиту доступа в Интернет с оконечных устройств, установленных как в помещениях Организации, так и вне их. Это позволяет осуществлять контроль за доступом в Интернет с оконечных устройств путем обеспечения проверки веб-сайтов, фильтрации файлов и защиты от вредоносных программ.

(c) **Сканирование уязвимости приложений.** Такое сканирование позволит проводить последовательную и более эффективную оценку безопасности мобильных и веб-приложений в процессе их разработки, тестирования и использования. Задача состоит в том, чтобы выявить уязвимости системы, сети и приложений.

(d) **Брандмауэр веб-приложений.** Эта программное обеспечение относится к новому поколению защиты веб-приложений и предоставления к ним доступа. Брандмауэр веб-приложений выступает в качестве защитного экрана и шлюза, который находится между веб-приложениями и Интернетом и защищает приложения от кибератак. Доступ извне отслеживается, фильтруется и контролируется.

(e) **Отслеживание уязвимостей.** Это направление предусматривает создание онлайновой автоматической системы верификации и отчетности, которая будет интегрирована с процессами управления инцидентами, изменениями и внесением исправлений. Это облегчит устранение уязвимостей, связанных с использованием необновленных систем и приложений.

(f) **Управление привилегированным доступом.** Это направление предусматривает не только информирование Организации о потенциальных угрозах, возникающих в связи с предоставлением различных видов привилегированного доступа, но и обеспечение защиты от злоупотреблений высокопривилегированными учетными записями (например, системных администраторов) благодаря использованию соответствующих инструментов.

(g) **Разграничения в рамках распределения полномочий.** Это направление предусматривает четкое разделение полномочий и ролей в рамках предоставления доступа к системам. Следует исключить случаи, в которых какое-либо лицо может

инициировать и подтверждать операции в целях совершения киберпреступлений (кражи или мошенничества в целях получения личной выгоды).

(h) **Технология введения в заблуждение.** Это направление предусматривает создание ловушек и ложных объектов в целях введения в заблуждение структур, использующих киберугрозы, и создания у них впечатления, что они закрепились в электронной системе Организации (например, с целью кражи учетных данных или секретов). Это позволит повысить возможности Секретариата по обнаружению действий внешних нарушителей и использовать эти знания для укрепления безопасности своих систем.

13. Сохранение положительной динамики имеет решающее значение. Включение этих направлений работы в общие усилия Секретариата по обеспечению кибербезопасности еще больше повысит эффективность методов идентификации, обнаружения, предупреждения, защиты и реагирования, обеспечивающих выполнение задач, предусмотренных дорожной картой по обеспечению кибербезопасности.

УСТОЙЧИВОЕ ФИНАНСИРОВАНИЕ

14. В соответствии с решением WHA70(16) (2017 г.) Генеральный директор уполномочен, при наличии возможности, выделять до конца каждого двухгодичного периода не менее 15 млн долл. США в Фонд инфраструктуры в виде инвестиций в информационные технологии[1]. Действующая программа по обеспечению кибербезопасности финансируется из средств Инфраструктурного фонда.

15. Секретариат считает обеспечение кибербезопасности одним из главных приоритетов. Важно сохранить результаты всех предпринятых до настоящего времени усилий и продолжить работу по защите Организации. В целях выполнения программы кибербезопасности была составлена первоначальная смета расходов. Однако поддержка мероприятий по обеспечению кибербезопасности после завершения программы также потребует вложения значительных средств в предстоящие годы.

16. Независимый консультативный надзорный комитет экспертов рекомендовал провести в рамках общего цикла планирования общий обзор расходов Организации в связи с деятельностью в области ИТ[2]. В ходе обзора следует проанализировать затраты как на управление деятельностью Секретариата, так и на реализацию всех инициатив по осуществлению изменений в области ИТ, включая кибербезопасность. Секретариат проводит этот обзор в более широком контексте подготовки предлагаемого программного бюджета на 2022-2023 гг.

[1] См. документ WHA70/2017/REC/1.

[2] См. документ EBPBAC30/2.

17. Секретариат предоставит государствам-членам в ходе тридцать четвертого совещания Комитета по программным, бюджетным и административным вопросам информацию о показателе осуществления инициатив (то есть показателе соотношения принятых мер и соответствующих изменений), и в том числе обновленный общий обзор будущих расходов на ИТ.

ДЕЙСТВИЯ ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

18. Исполкому предлагается принять доклад к сведению.

= = =