GUVERNUL REPUBLICII MOLDOVA

ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОЛДОВА

ПОСТАНОВЛЕНИЕ
о Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы

№ 811 от 29.10.2015

Мониторул Официал № 306-310/905 от 13.11.2015

* * *

На основании положений Закона № 64-XII от 31 мая 1990 года о Правительстве (повторное опубликование: Официальный монитор Республики Молдова, 2002 г., № 131-133, ст.1018), с последующими изменениями и дополнениями, Правительство

ПОСТАНОВЛЯЕТ:

1. Утвердить Национальную программу кибербезопасности Республики Молдова на 2016-2020 годы (прилагается).

2. Министерствам и другим центральным административным органам представлять Министерству информационных технологий и связи каждые полгода, до 1 августа и 1 февраля, информацию о выполнении Национальной программы кибербезопасности Республики Молдова на 2016-2020 годы, в соответствии с установленными обязательствами.

3. Министерству информационных технологий и связи обобщать полученную информацию и представлять Правительству каждые полгода, до 1 сентября и 1 марта, отчет о выполнении Национальной программы кибербезопасности Республики Молдова на 2016-2020 годы.

4. Мониторинг и координацию процесса выполнения Национальной программы кибербезопасности Республики Молдова на 2016-2020 годы возложить на Министерство информационных технологий и связи.

ПРЕМЬЕР-МИНИСТР **Валериу СТРЕЛЕЦ**

Контрассигнуют:

министр информационных технологий и связи **Павел ФИЛИП**

министр внутренних дел **Олег БАЛАН**

министр обороны **Анатолие ШАЛАРУ**

№ 811. Кишинэу, 29 октября 2015 г.

Утверждена
Постановлением Правительства
№ 811 от 29 октября 2015 г.

НАЦИОНАЛЬНАЯ ПРОГРАММА КИБЕРБЕЗОПАСНОСТИ РЕСПУБЛИКИ МОЛДОВА НА 2016-2020 ГОДЫ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Целью Национальной программы кибербезопаности Республики Молдова на 2016-2020 годы (в дальнейшем – *Программа*) является создание системы менеджмента

кибербезопасности Республики Молдова путем обеспечения безопасности услуг информационного общества, способствуя, таким образом, развитию экономики, основанной на знаниях, что в свою очередь будет стимулировать рост уровня экономической конкурентоспособности, социального единства, а также обеспечит создание новых рабочих мест.

2. Термины, использованные в Программе, имеют следующие значения:

1) *киберугроза* – обстоятельство или событие, которое представляет потенциальную угрозу для кибербезопасности;

2) *киберзащита* – действия, проведенные с целью защиты, мониторинга, анализа, обнаружения, противодействия агрессиям и обеспечения своевременного реагирования на угрозы кибернетическим инфраструктурам, предназначенным для национальной обороны;

3) *кибератака* – враждебное действие в киберпространстве, нарушающее кибербезопасность;

4) *аудит кибербезопасности* – системная, подробная, измеряемая и техническая оценка способа применения политик кибербезопасности на уровне кибернетических инфраструктур, а также составление рекомендаций по минимизации выявленных рисков;

5) *кибернетический инцидент* – событие, произошедшее в киберпространстве, последствия которого нарушают кибербезопасность;

6) *событие, произошедшее в киберпространстве,* – мероприятие, проведенное в киберпространстве, вследствие которого изменяется состояние кибернетических инфраструктур;

7) *кибернетические инфраструктуры* – инфраструктуры сферы информационных технологий и связи, состоящие из информационных систем, соответствующих приложений, сетей и услуг электронных коммуникаций;

8) *кибернетические инфраструктуры национального значения (КИНЗ)* – кибернетические инфраструктуры, которые поддерживают публичные услуги или услуги общественного значения, а также услуги информационного общества, нарушение которых может негативно повлиять на национальную безопасность или нанести серьезный ущерб государству или его гражданам;

9) *менеджмент идентичности* – методы подтверждения идентичности лиц в момент их доступа к определенным кибернетическим инфраструктурам;

10) *управление рисками* – сложный, непрерывный и гибкий процесс идентификации, оценки и противодействия рискам для кибербезопасности, основанный на использовании комплексных техник и инструментов для предотвращения потерь любого характера;

11) *операции в компьютерных сетях* – сложный процесс планирования, координации, синхронизации, согласования и проведения мероприятий в кибернетическом пространстве для защиты, контроля и использования компьютерных сетей с целью получения информационного превосходства при одновременной нейтрализации возможностей противника;

12) *устойчивость кибернетических инфраструктур* – способность составляющих частей кибернетических инфраструктур противостоять киберинциденту или кибератаке и восстановиться до нормального состояния;

13) *риск безопасности в киберпространстве* – вероятность того, что угроза материализуется, используя уязвимость, характерную для кибернетических инфраструктур;

14) *кибербезопасность* – нормальное состояние, возникшее вследствие применения комплекса проактивных и реактивных мер, посредством которых обеспечивается конфиденциальность, целостность, доступность, достоверность и невозможность отказа в доступе к информации в электронном формате, информационных систем и ресурсов, государственных и частных услуг в киберпространстве. Проактивные и реактивные меры включают в себя политики, концепции, стандарты и руководства по безопасности, управление рисками, деятельность по подготовке и информированию, внедрение

технических решений по защите кибернетических инфраструктур, менеджмент идентичности, менеджмент последствий;

15) *киберпространство* – виртуальное пространство, сгенерированное кибернетическими инфраструктурами, включая обработанное, сохраненное или переданное информационное содержание, а также действия, предпринятые пользователями в этой среде;

16) *уязвимость в киберпространстве* – неэффективность в проектировании и внедрении кибернетических инфраструктур или надлежащих мер безопасности, что может быть использовано с угрозой.

Другие термины в Программе используются в значении, определенном в Законе № 20-XVI от 3 февраля 2009 года о предотвращении и борьбе с преступностью в сфере компьютерной информации, Законе № 241-XVI от 15 ноября 2007 года об электронных коммуникациях и Законе № 467-XV от 21 ноября 2003 года об информатизации и государственных информационных ресурсах.

3. Концепция кибербезопасности основана на следующих принципах:

1) *защита прав и основных свобод человека*. Обеспечение кибербезопасности может быть целесообразным и эффективным только в случае, если оно основано на правах и основных свободах человека, в том числе на общечеловеческих ценностях. Никакой процесс передачи, обработки или хранения данных, в том числе персонального, коммерческого и конфиденциального характера, не может выполняться без использования информационных систем, сетей или услуг безопасных электронных коммуникаций. Любая обработка информации, выполненная с целью обеспечения кибербезопасности, должна соответствовать правовой основе и международным соглашениям, стороной которых Республика Молдова является;

2) *общедоступность*. Надежный и свободный доступ к интернету и его ресурсам является правом каждого лица. Ограниченный доступ или его отсутствие, а также цифровая неграмотность является недостатком как для граждан, так и для властей;

3) *кибернетическая устойчивость*. Предварительное или раннее выявление угроз и кибератак, других событий, происходящих в киберпространстве, является существенным из-за их трансграничного и ассиметрично материализующегося характера, они должны выявляться для устранения или смягчения последствий, которые могут повлиять на нормальное состояние кибербезопасности. Кибернетические угрозы возникают вследствие использования уязвимостей. Среда угроз и уязвимостей чрезвычайно изменчивая и динамичная: угрозы могут возникнуть в течение дней или даже часов. Следовательно, ответственные лица и координаторы по кибербезопасности должны непрерывно контролировать эту среду, выявлять киберугрозы и постоянно обращаться к признанным источникам информации компаний-лидеров в сфере кибербезопасности, экспертам научного сообщества и различным публикациям;

4) *совместное управление*. Киберпространство не может быть под контролем одной структуры как на местном или национальном, так и на региональном или глобальном уровне. В киберпространстве не могут быть установлены границы, аналогичные границам между административно-территориальными единицами или государствами. Таким образом, для обеспечения кибернетической устойчивости государственные власти и частный сектор должны развить необходимые навыки и эффективно сотрудничать. Посредством совместного управления и общих мероприятий государственные органы и частный сектор смогут успешно бороться с кибернетическими рисками и атаками, содействовать согласованными и эффективными мерами на события национального и межгосударственного значения, происходящие в киберпространстве;

5) *совместная ответственность и персональная ответственность за обеспечение кибербезопасности*. Растущая зависимость человеческой деятельности от информационных технологий и связи влечет за собой уязвимости, которые должны быть выявлены, тщательно проанализированы и удалены или уменьшены в зависимости от

потенциальной угрозы в адрес кибербезопасности. Все стороны, участвующие в выполнении мер по обеспечению кибербезопасности, будь то органы государственной власти, либо представители частного сектора или простые граждане, должны признать эту совместную ответственность и персональную ответственность, предпринимать собственные и совместные действия по защите, способствовать укреплению кибербезопасности и киберзащиты в соответствии с нормативно-правовой базой.

II. ТЕКУЩАЯ СИТУАЦИЯ И ОПРЕДЕЛЕНИЕ ОСНОВНОЙ ПРОБЛЕМЫ

4. Ускоренное развитие современных информационных и коммуникационных технологий поднимает на новый уровень подход к угрозам, рискам и уязвимостям в информационном обществе. В настоящее время на мировом уровне кибератаки возникают все чаще, они все сложнее и масштабнее, нанося огромный ущерб государственному, частному сектору и гражданам вследствие их асимметричного характера. Несанкционированный доступ к сетям и услугам электронных коммуникаций, неавторизированное изменение, удаление или повреждение информационных данных, нелегальное ограничение доступа к этим данным и кибершпионаж – проблемы мирового уровня. Угрозы и риски, атаки и кибернетические инциденты, а также другие события, происходящие в киберпространстве, материализуются путем использования уязвимостей человеческого, технического и процедурного характера. Экономические потери вследствие подобных уязвимостей весьма существенны.

5. Таким образом, в соответствии с докладами Нортон[1] за 2012 и 2013 годы, суммарная стоимость киберпреступлений растет. Общие потери в 2013 году составили около 113 миллиардов долларов по сравнению с 110 миллиардами долларов в 2012 году, а потери в среднем на одного пострадавшего составили 298 долларов США в 2013 году по сравнению с 197 долларами США в 2012 году. Согласно данным из тех же докладов мы постоянно подвержены значительным рискам при использовании незащищенных wi-fi сетей. Достаточно большой риск составляет несанкционированный доступ к личной электронной почте (54% в 2013 году по сравнению с 64% в 2012 году) вследствие перехвата пароля доступа, а также риск несанкционированного доступа к личным страницам пользователей социальных сетей (56% в 2013 году по сравнению с 63% в 2012 году). Достаточно высок и риск в электронной торговле, осуществляемой посредством онлайн-магазинов, доступ к которым осуществляется через незащищенные wi-fi сети (29% в 2013 году по сравнению с 31% в 2012 году). Вырос риск несанкционированного доступа к банковским счетам вследствие выполнения операций посредством незащищенных wi-fi сетей, который в 2013 году вырос до 29% по сравнению с 24% в 2012 году. Доступ к банковским счетам посредством незащищенных wi-fi сетей существенно увеличивает риск перехвата данных доступа, и, следовательно, дальнейший несанкционированный доступ к ним в преступных целях.

[1] Источник: https://symantec.com

6. Из-за достаточно высокого уровня вышеуказанных рисков доступа, а также других характерных кибернетических рисков в 2013 году число пострадавших от кибернетического мошенничества, кибератак и кибернетических происшествий насчитывает приблизительно 379 миллионов по сравнению с 558 миллионами пострадавших в 2012 году Таким образом, в 2013 году пострадали 64% владельцев мобильных устройств, 63% пользователей социальных сетей, 68% пользователей публичных wi-fi сетей, 65% родителей детей и 68 % развивающихся рынков. Несмотря на очень большое число пострадавших, только часть пользователей интернета осознает, что их электронные устройства (мобильные телефоны, планшеты, ноутбуки, компьютеры, и т.д.) могут быть подвержены кибератакам при их подключении к интернету, воздействие которых может быть существенно снижено, если соблюдать самые простые рекомендациям по безопасности. Именно этот факт значительно способствует росту

кибернетической (информационной) преступности, эксплуатируя уязвимость человеческого характера.

7. До настоящего времени не выполнено ни одного аудита по кибербезопасности, не существует исследований или отчетов, подробно отображающих ситуацию относительно информационной преступности в Республике Молдова, кибернетических угроз и рисков, кибернетических атак и происшествий, других событий, произошедших в киберпространстве, количества жертв и экономических потерь вследствие их материализации.

8. Единственным официальным источником статистических данных об информационной преступности является Регистр учета преступлений, уголовных дел, лиц, совершивших преступления, и материалов о преступлениях в рамках Автоматизированной интегрированной информационной системы учета преступлений, уголовных дел и лиц, совершивших преступления. Согласно информации из Автоматизированной информационной системы «Регистр криминалистической и криминологической информации», предоставленной Министерством внутренних дел, начиная с 2013 года и до августа 2015 года включительно, зарегистрировано 72 информационных преступления по статьям 208[1] и 259-261[1] Уголовного кодекса Республики Молдова, с материальным ущербом в размере около 21588 тысяч леев. В частности вследствие действий Генеральной прокуратуры и Генерального инспектората полиции были в 2013 году зарегистрированы 23 преступления с ущербом около 14139 тысяч леев, в 2014 году – 24 преступления с ущербом около 1 323 тысяч леев, а за первые 8 месяцев 2015 года – 25 преступлений с ущербом приблизительно в 6126 тысяч леев. Одновременно в этот же период времени зарегистрировано 57 нарушений авторского права и смежных прав на общую сумму наложенных штрафов приблизительно 99 тысяч леев. Несмотря на то, что данные из Регистра криминалистической и криминологической информации еще не полные и не отображают все категории преступлений и правонарушений в понимании Будапештской конвенции Совета Европы о киберпреступности, можно констатировать, число информационных преступлений и правонарушений растет.

9. В то же время, по данным Центра специальных телекоммуникаций, в 2014 году по сравнению с 2013 годом количество кибератак на web-серверы увеличилось на 26%, а уязвимость открытых портов – приблизительно на 385%. Вероятность заражения компьютеров информационными вирусами увеличилась приблизительно на 27%. Число инцидентов относительно электронной правительственной почты в 2014 году уменьшилось на 1% по сравнению с 2013 годом. В то же время снизилась доля этих инцидентов в общем количестве кибератак. В 2014 году эта доля снизилась до 40% по сравнению с 51% в 2013 году.

10. Высокая опасность материализации этих событий, произошедших в киберпространстве, в котором не существует границ, принудила ряд стран начиная с 2009 года включить в повестку дня в качестве доминирующего вопрос кибербезопасности. Уже 56 государств утвердили документы политик[2] в сфере кибербезопасности, в том числе 21 государство Европейского Союза. 37 государств мира утвердили документы политик в течение 2013-2015 годов, в том числе 14 государств – в 2015 году.

[2] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

11. Внутренняя нормативно-правовая база этих стран приведена в соответствие с положениями Конвенции Совета Европы о киберпреступности, утвержденной в Будапеште 23 ноября 2001 года с учетом Рекомендаций Международного союза электросвязи, касающихся кибербезопасности.

12. Республика Молдова ратифицировала Конвенцию Совета Европы о киберпреступности Законом № 6-XVI от 2 февраля 2009 года. В то же время принят Закон

№ 20-XVI от 3 февраля 2009 года о предупреждении и борьбе с преступностью в сфере компьютерной информации, внесены изменения и дополнения в Уголовный кодекс в соответствии с положениями ратифицированной конвенции, но ее положения процедурного характера, а также положения, касающиеся развития точки контакта сети 24/7, еще не внедрены.

13. В результате проведенного анализа выявлена основная проблема – отсутствие системы менеджмента кибербезопасности, в рамках которой согласованно выполнялись планирование и использование доступных ресурсов, определение уязвимостей и рисков вследствие аудита кибербезопасности, вмешательства, необходимые для уменьшения пагубного воздействия кибернетических преступлений, атак и инцидентов на устойчивое развитие информационного общества. Эта система должна распространяться на все сферы социальной, экономической и политической жизни страны. Ее необходимо создать и внедрить соответствующим структурам государственной и частной сферы.

14. Отсутствие системы менеджмента кибербезопасности Республики Молдова генерирует и отсутствие полных, достоверных, обновленных и структурированных статистических данных, что в свою очередь накладывает некоторые ограничения на выполненный анализ и определение оптимальных решений. От результата решения основной проблемы зависит эффективность мер, предпринятых ввиду развития безопасного информационного общества в Республике Молдова, технологического и научного прогресса, активного участия граждан в социальной и культурной жизни, а также динамика экономического роста страны.

15. До настоящего времени не существует законодательной базы относительно разграничения и согласования компетенций и ответственностей государственных и частных учреждений в области кибербезопасности, не применяется обязательный механизм аудита кибербезопасности, посредством которого могут быть выявлены кибернетические уязвимости, риски и угрозы с целью предотвращения или уменьшения при помощи специальных мер воздействия произошедших в киберпространстве атак, инцидентов и других событий, происхождение которых трудно определить.

16. Помимо правовых, нормативных и технически-нормативных регламентов существует ряд конкретных проблем, касающихся обеспечения кибербезопасности Республики Молдова, которые являются составными частями основной проблемы, установленной выше:

1) не обеспечена полная безопасность при обработке, хранении и доступе к данным, независимо от их классификации;

2) безопасность и целостность сетей и услуг электронных коммуникаций не приведены в соответствие со стандартами и рекомендациями Европейского Союза, Международного союза электросвязи, с положениями Соглашения об ассоциации между Республикой Молдова и Европейским Союзом;

3) недостаточный потенциал для предупреждения и срочного реагирования на национальном уровне (CERT) с учетом ассиметричного характера кибернетических атак и инцидентов;

4) национальная законодательно-нормативная база не в полной мере приведена в соответствие с положениями Конвенции Совета Европы о киберпреступности, компетентные учреждения не располагают четкими компетенциями касательно обеспечения кибербезопасности;

5) низкая способность кибероборонь вследствие ассиметричного характера кибератак;

6) не обеспечено непрерывное образование, обучение и информирование в сфере кибербезопасности;

7) недостаток международного сотрудничества и взаимодействия относительно выявления рисков, уязвимостей, других событий, происходящих в мировом киберпространстве, и предупреждения трансграничных кибернетических угроз и атак.

17. Решение основной проблемы, в том числе специфических проблем, предполагает внесение корректировок в законодательную и институциональную базу, нормативную и технически-нормативную базу, в непрерывную подготовку и сертификацию специалистов в сфере кибербезопасности, аудита кибербезопасности структур, которые обладают кибернетическими инфраструктурами, информационными системами и сетями электронных коммуникаций, в том числе тех, которые предоставляют информационные услуги и услуги электронных коммуникаций.

18. При этом решение указанных проблем соответствует общей горизонтальной цели относительно обеспечения кибербезопасности в рамках Национальной стратегии развития информационного общества «Цифровая Молдова 2020», утвержденной Постановлением Правительства № 857 от 31 октября 2013 года, положениями Соглашения об ассоциации между Республикой Молдова и Европейским Союзом, ратифицированного Законом № 112 от 2 июля 2014 года, а также новым видением Стратегии национальной безопасности Республики Молдова.

III. ЦЕЛИ ПРОГРАММЫ

19. Основной целью Программы, установленной вследствие проведенного анализа и определения основной проблемы, является создание и внедрение системы менеджмента кибербезопасности Республики Молдова, обеспечивающей соответствующим структурам публичной и частной сферы планирование и использование доступных ресурсов, определение вмешательств, необходимых для понижения пагубного воздействия кибернетических преступлений, атак и инцидентов на устойчивое развитие информационного общества.

20. Достижение основной цели Программы, в соответствии с проблемами, определенными в предыдущей главе, произойдет путем комплексного выполнения 7 специфических задач:

1) обработка, хранение и доступ к данным, в том числе к публичным данным;

2) безопасность и целостность сетей и услуг электронных коммуникаций;

3) развитие потенциала по предупреждению и срочному реагированию на национальном уровне (национальная сеть CERT);

4) предотвращение и борьба с киберпреступностью;

5) укрепление потенциала по киберзащите;

6) непрерывное обучение, подготовка и информирование в области кибербезопасности;

7) международное сотрудничество и взаимодействие в сферах, касающихся кибербезопасности.

IV. ДЕЙСТВИЯ, КОТОРЫЕ НЕОБХОДИМО ВЫПОЛНИТЬ ДЛЯ ДОСТИЖЕНИЯ ЦЕЛЕЙ

21. Для достижения целей, сформулированных в предыдущей главе, совместно с соответствующими структурами определен ряд действий, подлежащих выполнению, которые – для удобства и в соответствии со специфическими задачами – систематизированы в виде Плана действий по внедрению Национальной программы по кибербезопасности Республики Молдова (в дальнейшем – *План действий*).

22. Согласно Плану действий (приложение к настоящей Программе), специфическая задача «Обработка, хранение и доступ к данным, в том числе публичным данным» будет достигнута путем корректировки нормативно-правовой базы относительно кибербезопасности Республики Молдова, классификации типов информации, анализа и разработки предложений по применению на национальном уровне стандартов, относящихся к безопасной обработке, хранению и доступу к данным, определения методологии для оценки уязвимостей информационных систем на основе ранее установленных стандартов, разработки минимальных обязательных требований

кибербезопасности, сертификации специалистов, выполнения аудита кибербезопасности с разработкой планов по устранению выявленных уязвимостей, выполнение других мер согласно Плану действий.

23. Специфическая задача «Безопасность и целостность сетей и услуг электронных коммуникаций» будет достигнута путем согласования законодательства в сфере электронных коммуникаций с рамочными директивами Европейского Союза в данной сфере, установления минимальных мер безопасности, которые должны быть предприняты поставщиками для обеспечения безопасности и целостности сетей и услуг электронных коммуникаций, с сообщением об инцидентах, оказывающих воздействие на эти сети и услуги, применения на национальном уровне, европейских и международных стандартов относительно защиты и безопасности сетей электронных коммуникаций, в том числе путем выполнения других мер согласно Плану действий.

24. Специфическая задача «Развитие потенциала по предупреждению и срочному реагированию на национальном уровне (национальная сеть CERT)» будет достигнута путем создания Национального центра реагирования на инциденты кибербезопасности (CERT) и ведомственных центров в центральных органах публичного управления, органах местного публичного управления, других структурах, которые обладают информационными государственными системами, установления обязательств по обязательной оперативной отчетности и учету инцидентов киберзащиты для центральных и местных органов публичного управления и деловой среды в области информационных технологий и связи, разработки и применения методов раннего предотвращения инцидентов кибербезопасности Республики Молдова, проведения практических занятий и тренировок по укреплению способностей реагирования на кибернетические инциденты и атаки с их блокированием, в том числе путем проведения других мероприятий согласно Плану действий.

25. Специфическая задача «Предотвращение и борьба с киберпреступностью» будет достигнута путем разработки проектов законов для дальнейшего согласования уголовно-процессуального и административного законодательства с положениями Европейской конвенции о киберпреступности и решениями Комитета этой Конвенции, ратификации Дополнительного протокола к этой Конвенции, согласования законодательства и национальной статистики с положениями Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия и Дополнительного протокола к этой Конвенции, консолидации потенциала по предупреждению и борьбе с киберпреступностью в рамках Генеральной прокуратуры, Службы информации и безопасности, Генерального инспектората полиции Министерства внутренних дел, обучения сотрудников правоохранительных органов в области кибербезопасности в соответствии с рекомендациями проекта EAP Совета Европы, в том числе путем осуществления других мер согласно Плану действий.

26. Специфическая задача «Укрепление потенциала по киберзащите» будет достигнута путем установления ответственных органов и взаимного сотрудничества в мирное время, во время осады и войны в киберпространстве, путем разработки раздела киберзащиты Республики Молдова как составляющей части Стратегии информационной безопасности Республики Молдова, обучения в сфере кибербезопасности персонала в сфере национальной безопасности и обороны, развития военных возможностей защиты критической инфраструктуры и услуг, касающихся национальной обороны, осуществления других мер, согласно Плану действий.

27. Специфическая задача «Непрерывное образование, обучение и информирование в сфере кибербезопасности» будет достигнута путем создания лаборатории кибербезопасности, дополнения куррикулума, изучения учебного материала в области кибербезопасности, разработки и внедрения концепции кампаний по информированию и осознанию рисков в киберпространстве, установления требований по компетенции в сфере кибербезопасности персонала публичного и частного сектора, учета, обучения,

оценки и сертификации этого персонала, организации и проведения тренингов и семинаров в сфере кибербезопасности для персонала учреждений, содержащих элементы критической кибернетической инфраструктуры, осуществления других мер согласно Плану действий.

28. Специфическая задача «Международное сотрудничество и взаимодействие в сферах, касающихся кибербезопасности» будет достигнута путем создания Центра передового опыта для исследований и развития в сфере кибербезопасности, установления и развития отношений с международным сообществом по исследованиям в конкретных областях, которые лежат в основе кибербезопасности, развития сотрудничества между публичным и частным сектором относительно определения общих решений по кибербезопасности, внедрения мер по оценке угроз и рисков по отношению к установленным кибернетическим уязвимостям, заключения соглашений о международном сотрудничестве с европейскими, североатлантическими, национальными командами типа CERT других стран, осуществления других мер, согласно Плану действий.

V. ЭТАПЫ, СРОКИ И ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ

29. Программа не предусматривает поэтапную реализацию. Но по истечении каждого года внедрения будет осуществляться промежуточная оценка, в рамках которой промежуточные результаты будут анализироваться и сопоставляться с ожидаемыми, будет определяться уровень внедрения Программы. На основе выводов из Отчетной информации мониторинга и оценки (ОИМО), в случае необходимости, будут предлагаться корректировки целей и/или ожидаемых результатов, новые действия, актуализация Программы и/или Плана действий.

30. В Плане действий, прилагаемом к Программе, мероприятия сгруппированы согласно специфическим задачам, которые необходимо выполнить. В соответствующих рубриках Плана действий установлены ответственные за исполнение мер, соисполнители и сроки исполнения для получения ожидаемого результата. Первое учреждение в списке ответственных считается «главным ответственным» за исполнение мероприятия, оно координирует действия соисполнителей и других ответственных, привлекает партнеров по развитию для достижения ожидаемого результата в срок, установленный для действия.

VI. ОБЩАЯ ОЦЕНКА РАСХОДОВ И ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

31. В соответствующих рубриках Плана действий указываются ожидаемые результаты и расчетная стоимость реализации каждого мероприятия в отдельности для достижения этих результатов. Источники финансирования включают ресурсы партнеров по развитию и бюджетные средства.

32. Так, расчетная стоимость для достижения ожидаемых результатов, подытоженная по отдельным мероприятиям в рамках каждой программной цели, составляет:

1) обработка, хранение и безопасный доступ к данным, в том числе данным, представляющим общественный интерес – около 9504 тысяч леев;

2) безопасность и надежная целостность сетей и услуг электронных коммуникаций – около 1944 тысяч леев;

3) развитие потенциала по предупреждению и срочному реагированию на национальном уровне (национальная сеть CERT) – около 49608 тысяч леев;

4) предотвращение и борьба с киберпреступностью – около 2916 тысяч леев;

5) укрепление кибернетической обороноспособности – около 2232 тысяч леев.

6) непрерывное образование, обучение и информирование в сфере кибербезопасности – около 10089 тысяч леев;

7) международное сотрудничество и взаимодействие в сферах, касающихся кибербезопасности – около 648 тысяч леев.

33. Предварительная расчетная стоимость внедрения Программы в полном объеме составляет 76941 тысяч леев. Ожидаемым результатом внедрения Программы является система менеджмента кибербезопасности Республики Молдова, созданная и внедренная в соответствующих структурах государственной и частной сферы, которая обеспечит планирование и использование имеющихся ресурсов, выявление необходимых мер в целях снижения пагубного воздействия киберпреступности, кибератак и киберинцидентов на устойчивое развитие информационного общества. Эта система будет распространяться во всех сферах социальной, экономической и политической жизни страны.

VII. ПОКАЗАТЕЛИ ПРОГРЕССА И ДОСТИЖЕНИЙ

34. Область кибербезопасности, будучи относительно новой в мире, еще не имеет показателей прогресса и достижений, рекомендованных для мониторинга и оценки внедрения документов политик в данной области. Тем не менее, исходя из необходимости мониторинга и оценки внедрения Программы, будут применены в комплексе 17 показателей результата (ПР):

ПР1 – доля разработки проектов законодательных и нормативных актов, документов политик и технических документов (рассчитанная в процентах от их общего количества), предусмотренных в Плане действий;

ПР2 – доля отчетов (информации) о выполненных мониторинге и оценке (рассчитанная в процентах от их общего количества), предусмотренных в Программе;

ПР3 – количество мер, выполненных в рамках Плана действий (до, после установленных сроков и в установленные сроки);

ПР4 – количество рекомендаций по предотвращению рисков и снижению киберуязвимостей;

ПР5 – количество разработанных технических предписаний и проектов стандартов по кибербезопасности;

ПР6 – число организаций, которые воспользовались возможностью обучения сотрудников обеспечению кибербезопасности, число лиц, которые прошли это обучение;

ПР7 – число организаций, в которых был проведен внешний/внутренний аудит кибербезопасности с целью выявления киберрисков и киберуязвимостей на уровне организаций;

ПР8 – доля органов публичного управления, которые применяют собственные политики внутренней кибербезопасности;

ПР9 – доля центральных органов публичного управления, которые создали собственный ведомственный CERT в национальной сети CERT;

ПР10 – количество организаций-участников Системы менеджмента кибербезопасности Республики Молдова;

ПР11 – количество уголовных дел и дел по правонарушениям, относящихся к киберпреступности, зарегистрированных в Автоматизированной информационной системе «Регистр криминалистической и криминологической информации», число лиц, совершивших эти преступления и/или правонарушения, число пострадавших людей, объем ущерба, причиненного пострадавшими, объем наложенных штрафов;

ПР12 – количество исследований и обзоров, проведенных в сфере кибербезопасности;

ИР13 – количество опубликованных рефератов/сообщений о кибербезопасности;

ПР14 – количество проведенных семинаров, круглых столов, тренингов, семинаров и других мероприятий по кибербезопасности, число участников этих мероприятий;

ПР15 – количество практических рекомендаций по повышению уровня информирования населения о киберрисках и киберугрозах, обеспечение кибербезопасности по месту жительства;

ПР16 – число информационных кампаний, организованных соответствующими учреждениями в сфере кибербезопасности;

ПР17 – объем информации (отчеты о мониторинге и оценке, информационные справки и т.д.), опубликованной на официальном веб-сайте Министерства информационных технологий и связи.

35. Чтобы определить прогресс и достижения текущего и окончательного внедрения, показатели результата периодически будут сопоставляться с показателями Национальной стратегии развития информационного общества «Цифровая Молдова 2020», с текущими результатами выполнения Соглашения об ассоциации между Республикой Молдова и Европейским Союзом, с рекомендациями Международного союза электросвязи, рекомендациями партнеров по развитию.

VIII. ПРОЦЕДУРЫ ОТЧЕТНОСТИ И ОЦЕНКИ

36. Процедуры отчетности и оценки направлены на максимизацию эффектов, достигнутых вследствие реализации Программы в соответствии с ожидаемыми результатами, указанными в рубрике «Показатель результата» Плана действий.

37. Процесс внедрения Программы сопровождается непрерывным мониторингом на институциональном, национальном и международном уровнях выполнения намеченных действий и реально полученных результатов, чтобы, в случае необходимости, были внесены соответствующие изменения в продвигаемые публичные политики и предпринимаемые действия, а также согласованием целей и мер Плана действий с результатами, ожидаемыми от реализации Программы, в целях проведения наиболее точной оценки процесса реализации Программы.

38. В рамках процесса мониторинга составляется Отчетная информация о мониторинге и оценке, которая включает релевантные данные о результатах выполнения задач Программы и выполнении соответствующих мер Плана действий, согласованных с результатами внедрения Национальной стратегии развития информационного общества «Цифровая Молдова 2020». К данной информации прилагаются отчеты о достижениях, отчеты об оценке и/или пояснительные записки с выводами и предложениями. В частности, процесс мониторинга и оценки направлен на содействие анализу текущей ситуации и тенденций в достижении целей Программы, анализу выполнения Плана действий и точной оценке текущих и конечных результатов, достигнутых по сравнению с ожидаемыми результатами.

39. На уровне международных организаций-доноров (партнеров по развитию), финансирующих некоторые этапы, составные части или комплексы мер в рамках Программы, отчетность и мониторинг будут соответствовать их требованиям. Периодические отчеты о ходе реализации, информационные справки и отчеты об оценке будут составляться в формате, одобренном соответствующим донорским финансовым учреждением и Правительством.

40. На национальном уровне процедуры отчетности и оценки выполняются Министерством информационных технологий и связи на основании Отчетной информации о мониторинге и оценке, представляемой каждое полугодие главными ответственными за выполнение мер из Плана действий. За каждый год внедрения Министерство информационных технологий и связи, в сотрудничестве с главными ответственными, указанными в Плане действий, и другими заинтересованными учреждениями, составляет годовой отчет об оценке внедрения Программы, который представляется Правительству и Межсекторальному совету по кибербезопасности до 1 марта следующего года. В зависимости от случая, Министерство информационных технологий и связи, на основании результатов промежуточной или полугодовой оценки, представляет на рассмотрение и утверждение проекты постановлений Правительства по актуализации Программы и/или Плана действий.

41. На институциональном уровне процедуры отчетности и оценки осуществляются каждое полугодие учреждениями, ответственными за меры, предусмотренные в Плане действий. Главное ответственное учреждение за выполнение меры составляет Отчетную

информацию о мониторинге и оценке реализации меры, за которую несет ответственность, и представляет эту информацию Министерству информационных технологий и связи до 1 августа и 1 февраля следующего семестра. В случае необходимости, главное ответственное учреждение за выполнение меры, создает рабочую группу из представителей ответственных учреждений и соисполнителей, партнеров по развитию, других профильных учреждений в целях организации и эффективного выполнения соответствующей меры, согласно утвержденному плану работы. Факт создания рабочей группы и утверждения плана работы по выполнению меры отражается в Отчетной информации о мониторинге оценки.

42. Оценка осуществляется путем сравнения реально достигнутых результатов с ожидаемыми результатами за соответствующий отчетный период. В зависимости от ситуации, оценка может проводиться путем исследований и обзоров, в сотрудничестве с заинтересованными учреждениями, указанными в Плане действий.

43. По истечении каждого года внедрения Программы осуществляется промежуточная оценка, а по завершении ее внедрения – итоговая оценка. В рамках промежуточной оценки анализируются промежуточные результаты по сравнению с ожидаемыми результатами. После выводов и предложений, изложенных в Отчете об оценке внедрения Программы, в случае необходимости, предлагаются корректировки задач и/или ожидаемых результатов, новые меры, актуализация Программы и/или Плана действий.

44. В конце 2020 года составляется Итоговый отчет об оценке внедрения Программы, в котором отражаются реализация задач Программы, выполнение мер, предусмотренных в Плане действий, в том числе влияние внедрения Программы на кибербезопасность Республики Молдова. Итоговый отчет должен включать выводы и предложения по развитию и распространению результатов внедрения в других сферах социальной, экономической и политической жизни страны.

45. Министерство информационных технологий и связи информирует общественность о ходе внедрения Программы путем размещения на своем официальном сайте пресс-релизов о действиях по внедрению Программы, полугодовых, годовых и конечных результатах, достигнутых в ходе ее внедрения, а также путем предоставления соответствующей информации местным и зарубежным партнерам.

46. В процессе мониторинга важная роль отводится гражданскому обществу, которое должно:

1) активно участвовать в качестве социального наблюдателя за выполнением настоящей Программы, в том числе путем обобщения и распространения независимой информации о показателях реального прогресса, а также путем информирования о накопленном передовом опыте и выявленных недостатках;

2) участвовать в социальном диалоге с Правительством, в частности с Министерством информационных технологий и связи, другими центральными административными органами и предлагать новые решения по повышению эффективности внедрения Программы.

Приложение
к Национальной программе кибербезопасности
Республики Молдова на 2016-2020 годы

ПЛАН ДЕЙСТВИЙ
по внедрению Национальной программы кибербезопасности Республики Молдова на 2016-2020 годы

№	Действие	Ответственные	Партнеры	Срок и/или	Показатель	Источники

п/п		учреждения		период исполнения	результата	финансирования, оценочная стоимость леев
1	2	3	4	5	6	7
1.	**Обработка, хранение и безопасный доступ к данным, в том числе к публичным данным.** Оценочная стоимость – 9504 тыс.леев					
1.1.	Обеспечение приведения в соответствие нормативно-законодательной базы по кибербезопасности Республики Молдова, которая будет предусматривать: a) определение терминов (понятий) в области кибербезопасности; b) разграничение компетенций по сферам; c) установление органа с функциями по мониторингу соблюдения требований кибербезопасности; d) назначение органа, уполномоченного контролировать внедрение результатов аудита в области кибербезопасности; e) обязательства держателей государственных информационных систем по периодическому проведению аудита этих систем, с установлением периодичности, уровней, и представлением отчета компетентному органу; f) санкции за	Министерство информационных технологий и связи, Служба информации и безопасности	Государственная канцелярия, Министерство внутренних дел, Министерство обороны, Генеральная прокуратура, Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий, Национальный центр по защите персональных данных	2016-2017 годы	Проект закона, разработанный и направленный на рассмотрение Правительству	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 2592 тыс.

	несоблюдение аудиторского заключения о соответствии минимальным обязательным требованиям кибербезопасности; g) персональную ответственность за обеспечение кибербезопасности; h) введение в государственные органы функции координатора по кибербезопасности, в том числе его основных обязанностей; i) создание межотраслевого совета по вопросам кибербезопасности (с функцией по координации деятельности кибербезопасности)					
1.2.	Классификация типов информации, за исключением государственной тайны	Министерство информационных технологий и связи	Служба информации и безопасности, Министерство внутренних дел, Генеральная прокуратура, Национальный центр по защите персональных данных, Центр специальных телекоммуникаций	2016 год	Утвержденная классификация	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
1.3.	Анализ и разработка предложений по применению на национальном уровне стандартов, связанных с обработкой, хранением и безопасным доступом к данным в соответствии с классификацией типов информации, рассмотренных в	Министерство информационных технологий и связи, Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий	Национальный институт стандартизации, Центр специальных телекоммуникаций, Министерство внутренних дел, Министерство обороны, Служба информации и безопасности, Национальный центр по защите персональных	2016-2017 годы	Предложения по применению европейских и международных стандартов, связанных с обработкой, хранением и безопасным доступом к данным	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию, ориентировочная стоимость – 216 тыс.

	рамках технических комитетов по стандартизации ТК 28 «Информационные технологии» и ТК 29 «Электронные коммуникации»		данных, технические комитеты по стандартизации ТК 28 «Информационные технологии» и ТК 29 «Электронные коммуникации»			
1.4.	Разработка методологии для оценки уязвимости государственных информационных систем на основе определенных, перенятых и утвержденных стандартов	Министерство информационных технологий и связи, Служба информации и безопасности, Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий	Национальный институт стандартизации, Государственная канцелярия, Министерство внутренних дел, Министерство обороны, технические комитеты по стандартизации ТК 28 «Информационные технологии» и ТК 29 «Электронные коммуникации»	2016-2017 годы	Методология, разработанная и утвержденная постановлением Правительства	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
1.5.	Разработка обязательных минимальных требований кибербезопасности	Министерство информационных технологий и связи	Министерство обороны, Министерство внутренних дел, Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий, Служба информации и безопасности, Центр специальных телекоммуникаций, Национальный центр по защите персональных данных	2016-2017 годы	Обязательные минимальные требования кибербезопасности, утвержденные Правительством	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
1.6.	Сертификация специалистов исходя из определенных стандартов и методологий, и утвержденных обязательных	Министерство информационных технологий и связи	Государственная канцелярия, Служба информации и безопасности, Генеральная прокуратура, Министерство	2016-2018 годы	Количество органов центрального и местного публичного управления, других ведомств,	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию.

	минимальных требований кибербезопасности		внутренних дел, Министерство обороны		являющихся держателями государственных информационных систем, для которых сертифицированы специалисты; число сертифицированных специалистов	Ориентировочная стоимость – 864 тыс.
1.7.	Определение и планирование в бюджетах учреждений финансовых средств, необходимых для проведения аудита кибербезопасности на основе утвержденной методологии	Министерство финансов, органы центрального местного публичного управления, держатели государственных информационных систем	Государственная канцелярия, Министерство внутренних дел, Генеральная прокуратура, Министерство обороны, Служба информации и безопасности	2016 год	Выделенные финансовые средства	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость не указана.
1.8.	Проведение аудита в органах центрального и местного публичного управления, других ведомствах, являющихся держателями государственных информационных систем, с целью выявления уязвимостей и соответствия обязательным минимальным требованиям кибербезопасности	Органы центрального и местного публичного управления, держатели государственных информационных систем	Министерство информационных технологий и связи	2017-2020 годы	Количество ведомств, в которых проведен аудит	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 864 тыс.
1.9.	Разработка плана по устранению уязвимостей согласно рекомендациям аудита и его выполнение под персональную ответственность в органах центрального и местного публичного управления, других ведомствах, являющихся держателями государственных информационных	Органы центрального местного публичного управления, держатели государственных информационных систем	Министерство информационных технологий и связи	2016-2018 годы	Количество ведомств, доложивших о реализации плана по устранению уязвимостей	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 1296 тыс.

	систем					
1.10.	Разработка и внедрение методологии маркировки информации, предоставленной системой, в которой содержатся персональные данные с использованием «временной метки»	Национальный центр по защите персональных данных	Министерство информационных технологий и связи, Служба информации и безопасности, Министерство внутренних дел, Центр специальных телекоммуникаций	2016-2019 годы	Разработанная и внедренная методология	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 216 тыс.
1.11.	Разработка и внедрение законодательных актов, необходимых для введения мер безопасности и обязательных стандартов в компаниях в области информационных технологий и коммуникаций с установлением обязательных минимальных требований безопасности государственных информационных систем и информации из этих систем	Министерство информационных технологий и связи, Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий	Государственная канцелярия, Министерство обороны, Служба информации и безопасности, Министерство внутренних дел	2017 год	Законодательные акты, разработанные и направленные на утверждение Правительству	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
2.	**Безопасность и целостность сетей и услуг электронных коммуникаций.** Ориентировочная стоимость – 1944 тыс.леев					
2.1.	Приведение законодательства в области электронных коммуникаций в соответствие с рамочными директивами ЕС в данной области	Министерство информационных технологий и связи, Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий	Служба информации и безопасности, Министерство внутренних дел, Министерство обороны, Центр специальных телекоммуникаций, Национальный центр по защите персональных данных	2016 год	Проект закона, разработанный и направленный на рассмотрение Правительству	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 216 тыс.
2.2.	Установление минимальных мер безопасности, которые должны принимать поставщики для	Национальное агентство по регулированию в области электронных коммуникаций	Министерство информационных технологий и связи	2016-2017 годы	Проект нормативного акта, утвержденный постановлением Административн	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы

	обеспечения безопасности, безотказности и целостности сетей и/или услуг электронных коммуникаций и предоставление отчета об инцидентах с существенным влиянием на них	и информационных технологий			ого совета Национального агентства по регулированию в области электронных коммуникаций и информационных технологий	партнеров по развитию Ориентировочная стоимость – 432 тыс.
2.3.	Анализ и внедрение на национальном уровне европейских и международных стандартов, относящихся к защите и безопасности сетей электронных коммуникаций и передача их на утверждение Национальному институту по стандартизации	Министерство информационных технологий и связи.	Национальный институт стандартизации, Технический комитет по стандартизации ТК 29 «Электронные коммуникации»	2016-2017 годы	Принятые стандарты	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
2.4.	Проведение исследования относительно внесения изменений в законодательство об электронных коммуникациях с целью устранения или уменьшения количества обезличенных абонентов услуг электронных коммуникаций	Служба информации и безопасности	Министерство информационных технологий и связи, Генеральная прокуратура, Министерство внутренних дел, Национальный центр по защите персональных данных	2016-2017 годы	Разработанное исследование	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
2.5.	Дальнейшее развитие специальной сети связи органов публичного управления на всей территории Республики Молдова	Государственная канцелярия, Служба информации и безопасности, Центр специальных телекоммуникаций	Министерство внутренних дел, Министерство обороны, Генеральная прокуратура, Министерство информационных технологий и связи	Согласно плану, утвержденному Правительством	Количество городов, охваченных сетью специальных телекоммуникаций	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
3.	**Создание центра реагирования на киберинциденты на национальном уровне (национальная сеть CERT).** Ориентировочная стоимость – 49608 тыс.леев					
3.1.	Создание Национального центра реагирования на	Государственная канцелярия, Министерство информационн	Генеральная прокуратура, Центр специальных	2016 год	Создан Национальный центр	Бюджет учреждений в пределах утвержденных

	киберинциденты (CERT)	ых технологий и связи, Министерство внутренних дел, Служба информации и безопасности	телекоммуникаций, Министерство обороны			ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 29700 тыс.
3.2.	Создание национальной системы оповещения и информирования о киберинцидентах в режиме реального времени	Государственная канцелярия, Центр специальных телекоммуникаций	Служба информации и безопасности, Министерство внутренних дел, Министерство обороны, Генеральная прокуратура	2016-2017 годы	Созданная функциональная система	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 594 тыс.
3.3.	Создание ведомственных центров реагирования на киберинциденты в органах центрального и местного публичного управления, других учреждениях, являющихся держателями государственных информационных систем	Органы центрального и местного публичного управления, держатели государственных информационных систем		2016-2017 годы	Количество созданных ведомственных центров	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 14850 тыс.
3.4.	Установление для органов центрального и местного публичного управления и предпринимательской среды в области информационных и коммуникационных технологий обязанностей по обязательному оперативному сообщению о киберинцидентах на основе механизма обмена данными и четко определенных ролей	Государственная канцелярия	Служба информации и безопасности, Министерство внутренних дел, Министерство обороны, Министерство информационных технологий и связи, Генеральная прокуратура, Центр специальных телекоммуникаций, Национальный центр по защите персональных данных	2016-2017 годы	Утвержденные обязанности	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
3.5.	Организация базы данных, с доступом ответственных	Государственная канцелярия	Генеральная прокуратура, Министерство внутренних дел,	Постоянно	Система, созданная в соответствии с утвержденной	Бюджет учреждений в пределах утвержденных

	органов, идентифицированных или зарегистрированных кибернетических угроз, уязвимостей и инцидентов, технологий и методов, используемых для атак, наилучших практик для защиты отрасли информационных и коммуникационных технологий		Служба информации и безопасности, Министерство обороны, Министерство информационных технологий и связи, Центр специальных телекоммуникаций, Национальный банк Молдовы, Главная государственная налоговая инспекция, Национальный центр по защите персональных данных		концепцией	ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 1800 тыс.
3.6.	Проведение совместных учений и тренировок для укрепления потенциала реагирования на кибератаки, в том числе блокирования симулированных кибератак	Государственная канцелярия, Служба информации и безопасности, Центр специальных телекоммуникаций	Министерство обороны, Министерство внутренних дел, Генеральная прокуратура, Министерство информационных технологий и связи	Постоянно	Количество организованных упражнений; количество проведенных тренировок; высокая способность реагирования на киберугрозы	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.
3.7.	Консолидация потенциала команды Национального центра реагирования на инциденты кибербезопасности для обеспечения стратегического анализа инцидентов безопасности и координации ответных действий на инциденты безопасности в государственном, частном и научном секторах, в том числе путем организации тренингов квалифицированными специалистами	Государственная канцелярия, Центр специальных телекоммуникаций.	Служба информации и безопасности, Министерство внутренних дел, Министерство обороны, Генеральная прокуратура	2016-2018 годы	Улучшенный потенциал	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.
3.8.	Разработка механизмов	Государственная канцелярия,	Служба информации и	2016-2018 годы	Методы (модели)	Бюджет учреждений в

	(моделей) раннего предупреждения инцидентов кибербезопасности в Республике Молдова, в том числе на основе государственно-частного партнерства	Центр специальных телекоммуникаций	безопасности, Министерство внутренних дел, Министерство обороны		раннего предупреждения инцидентов кибербезопасности	пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
4.	**Предотвращение и борьба с киберпреступностью.** Ориентировочная стоимость – 2916 тыс.леев					
4.1.	Разработка проекта закона о внесении изменений и дополнений в уголовное законодательство и законодательство о правонарушениях для предотвращения и борьбы с информационной кибербезопасностью в целях его непрерывной гармонизации с положениями Европейской конвенции об информационной преступности и решениями Комитета этой Конвенции	Министерство внутренних дел, Служба информации и безопасности, Генеральная прокуратура	Министерство обороны, Министерство информационных технологий и связи	2016 год	Проект закона о внесении изменений и дополнений в Уголовный кодекс, Уголовно-процессуальный кодекс и Кодекс об административных правонарушениях, разработанный и направленный на рассмотрение Правительству	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена.
4.2.	Обучение сотрудников правоохранительных органов, специалистов, сертифицированных в области кибербезопасности: a) обнаружению, расследованию, уголовному преследованию и судебному разбирательству информационных преступлений; b) связям между информационной преступностью, организованной преступностью, экономической преступностью и другими категориями	Национальный институт юстиции	Министерство внутренних дел, Служба информации и безопасности, Генеральная прокуратура	2016-2020 годы	Количество проведенных тренингов; количество обученных лиц	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.

	правонарушений					
4.3.	Внедрение рекомендаций Совета Европы, в частности, проекта EAP по подготовке персонала правоохранительных органов	Национальный институт юстиции, Академия им.Штефана чел Маре Министерства внутренних дел	Генеральная прокуратура, Министерство внутренних дел, Служба информации и безопасности, Технический университет Молдовы, Государственный университет Молдовы	2016 год	Учебный план, разработанный и внедренный	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.
4.4.	Разработка и утверждение проекта закона о ратификации Дополнительного протокола к Конвенции Совета Европы об информационной преступности	Министерство внутренних дел	Государственная канцелярия, Служба информации и безопасности, Генеральная прокуратура, Министерство иностранных дел и европейской интеграции	2016 год	Проект закона, разработанный и направленный на рассмотрение Правительству	Бюджет учреждений в пределах утвержденных ассигнований. Стоимость не определена.
4.5.	Приведение национального законодательства в соответствие с положениями Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия и Дополнительного протокола к Конвенции (Лансароте, 25 октября 2007 г.)	Министерство внутренних дел	Генеральная прокуратура	2016-2017 годы	Проект закона, разработанный и направленный на рассмотрение Правительству	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена.
4.6.	Проведение исследования для совершенствования нормативно-правовой базы в области предотвращения и борьбы с информационными преступлениями	Генеральная прокуратура, Министерство внутренних дел, Служба информации и безопасности	Государственная канцелярия, Министерство юстиции, Министерство информационных технологий и связи, Министерство обороны	2016 год	Проект поправок к нормативной базы, разработанный и направленный на рассмотрение Правительству	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 216 тыс.
4.7.	Укрепление в рамках Генеральной прокуратуры, Службы информации и безопасности и Генерального	Министерство внутренних дел, Служба информации и безопасности, Генеральная прокуратура		2016-2019 годы	Разработанный институциональный потенциал с составлением, по необходимости, предложений по внесению	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию.

	инспектората полиции Министерство внутренних дел потенциала по предотвращению и борьбе с информационной преступностью и, по необходимости, формирование предложений по внесению поправок в нормативно-правовую базу, а также создание лаборатории для тестирования и экспертизы				поправок в нормативно-правовую базу	Ориентировочная стоимость – 900 тыс.
5.	**Консолидация потенциала по киберзащите**. Ориентировочная стоимость – 2232 тыс.леев					
5.1.	Разработка раздела по киберзащите Республики Молдова, в качестве составной части Стратегии информационной безопасности Республики Молдова	Служба информации и безопасности, Министерство обороны, Министерство внутренних дел	Генеральная прокуратура	2016 год	Раздел, разработанный и представленный для включения в Стратегию информационной безопасности Республики Молдова.	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена.
5.2.	Установление ответственных органов и взаимное сотрудничество в мирное время, в ситуациях кризиса, осады и войны в киберпространстве	Служба информации и безопасности, Министерство обороны, Министерство внутренних дел	Государственная канцелярия, Центр специальных телекоммуникаций, Министерство просвещения, Министерство финансов, Министерство экономики, Министерство информационных технологий и связи, Генеральная прокуратура	2016-2017 годы	Проект закона, утвержденный и представленный Парламенту для принятия	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
5.3.	Использование возможностей киберпространства для продвижения национальных интересов, ценностей и целей в киберпространстве	Служба информации и безопасности, Министерство информационных технологий и связи	Министерство внутренних дел, Министерство обороны, Генеральная прокуратура, Национальный центр по защите персональных данных	2016-2018 годы	Политики, разработанные и утвержденные	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена.
5.4.	Развитие военного потенциала по	Министерство обороны	Служба информации и	2016-2017 годы	Разработанный потенциал	Бюджет учреждений в

	защите критической инфраструктуры и услуг, предназначенных для национальной обороны		безопасности, Министерство внутренних дел, Министерство информационных технологий и связи			пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.
5.5.	Определение программ по повышению осведомленности и обучению персонала, предназначенного для обеспечения национальной безопасности и защиты в области кибербезопасности	Служба информации и безопасности, Министерство обороны	Министерство внутренних дел, Министерство информационных технологий и связи, Министерство просвещения	2016-2017 годы	Обученный персонал	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.
5.6.	Установление отношений сотрудничества с национальными и международными учреждениями в данной области	Служба информации и безопасности, Министерство обороны	Министерство внутренних дел, Министерство иностранных дел и европейской интеграции, Министерство информационных технологий и связи	2016-2018 годы	Установленные процедуры сотрудничества	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена
6.	**Обучение, подготовка и непрерывное информирование в области кибербезопасности.** Ориентировочная стоимость – 10089 тыс.леев					
6.1.	Разработка концепции кампаний по информированию и осведомлению о рисках в киберпространстве	Государственная канцелярия, Министерство информационных технологий и связи	Министерство внутренних дел, Генеральная прокуратура, Служба информации и безопасности, Центр специальных телекоммуникаций, Центр электронного управления, Национальный центр по защите персональных данных	2016-2017 годы	Утвержденная концепция информационных кампаний	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.
6.2.	Дополнение учебного плана в области кибербезопасности	Министерство просвещения	Министерство информационных технологий и связи, Центр электронного управления, Технический университет Молдовы, Государственны	2016-2018 годы	Утвержденный учебный план	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость

			й университет Молдовы, Национальный центр по защите персональных данных			– 432 тыс.
6.3.	Создание портала с оперативным оповещением об угрозах в киберпространстве (цифровом пространстве)	Государственная канцелярия, Центр специальных телекоммуникаций	Министерство информационных технологий и связи	2016-2018 годы	Созданный функциональный портал.	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 900 тыс.
6.4.	Установление требований к компетенции в области кибербезопасности для персонала в государственном и частном секторе, а также организация процесса обучения, оценивания и сертификации специалистов в этой области	Министерство информационных технологий и связи	Служба информации и безопасности, Министерство внутренних дел, Генеральная прокуратура, Центр специальных телекоммуникаций, Министерство обороны	2016-2018 годы	Число сертифицированных специалистов	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 432 тыс.
6.5.	Организация и проведение тренингов и семинаров в области кибербезопасности для персонала государственного и частного сектора, держателей элементов критической инфраструктуры	Министерство информационных технологий и связи, Центр специальных телекоммуникаций	Служба информации и безопасности, Министерство внутренних дел, Генеральная прокуратура, Министерство обороны, Центр электронного управления, Технический университет Молдовы, Государственный университет Молдовы	Постоянно	Число проведенных тренингов и семинаров	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена
6.6.	Создание лаборатории кибербезопасности	Центр специальных телекоммуникаций, Технический университет Молдовы	Министерство информационных технологий и связи, Министерство обороны	2016-2018 годы	Созданная лаборатория	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 7425 тыс.
7.	**Международное сотрудничество и взаимодействие в сферах, касающихся кибербезопасности**. Ориентировочная стоимость - 648 тыс.леев					

7.1.	Заключение договоров о сотрудничестве с другими национальными командами реагирования на инциденты, связанные с кибербезопасностью (CERT), а также US–CERT, европейскими и Североатлантическими (NATO NCERT)	Государственная канцелярия, Министерство информационных технологий и связи, Министерство обороны	Служба информации и безопасности, Министерство внутренних дел, Генеральная прокуратура	2016-2018 годы	Количество заключенных соглашений	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена
7.2.	Создание платформы по координированию и консультированию в области оценивания киберугроз и поиска решений	Государственная канцелярия, Министерство информационных технологий и связи	Служба информации и безопасности, Министерство внутренних дел, Министерство обороны, Генеральная прокуратура, Центр специальных телекоммуникаций	2016-2018 годы	Платформа по координированию-консультированию разработанная и утвержденная	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Ориентировочная стоимость – 648 тыс.
7.3.	Развитие сотрудничества с частным сектором (определение приложений, необходимых для реализации мер безопасности; создание точек соприкосновения для обеспечения запроса данных и информации в соответствии с законными положениями и создание современной системы передачи запросов; проведение регулярных встреч в рамках дискуссионных форумов для лучшего осознания оперативной обстановки и понимания потребностей каждого учреждения)	Государственная канцелярия, Министерство информационных технологий и связи	Министерство внутренних дел, Служба информации и безопасности, Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий, Генеральная прокуратура	2016-2019 годы	Количество выявленных заявок; количество контактных пунктов; современная система передачи запросов; количество проведенных встреч	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена
7.4.	Продвижение	Министерство	Министерство	Постоянно	Национальные	Бюджет

	национальных интересов кибербезопасности в международных форматах сотрудничества, в которых участвует Республика Молдова	информационных технологий и связи, Министерство внутренних дел, Министерство обороны, Служба информации и безопасности, Генеральная прокуратура	иностранных дел и европейской интеграции, Государственная канцелярия, Центр специальных телекоммуникаций, Центр электронного управления		интересы, продвинутые в международных форматах сотрудничества	учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена
7.5.	Продвижение сотрудничества между университетами Молдовы с мировыми лидерами в обучении и сертификации в области кибербезопасности, такими как (ISC) 2, ISACA, SANS	Министерство просвещения.	Министерство информационных технологий и связи, Университеты Республики Молдова	Постоянно	Количество проведенных встреч	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена.
7.6.	Установление и развитие отношений с международным научным сообществом в определенных областях, являющихся основой кибербезопасности	Министерство просвещения, Академия наук Молдовы	Министерство иностранных дел и европейской интеграции, Министерство информационных технологий и связи, Институт развития электронного общества	2016-2019 годы	Количество установленных отношений	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена.
7.7.	Установление и развитие отношений с мировыми лидерами в области кибербезопасности для создания передового центра исследований и развития в Республике Молдова	Министерство просвещения	Министерство информационных технологий и связи, Академия наук Молдовы, Институт развития электронного общества	2016-2018 годы	Созданный передовой центр	Бюджет учреждений в пределах утвержденных ассигнований; ресурсы партнеров по развитию. Стоимость не определена

Hotrrorile Guvernului

811/29.10.2015 Hotrrore cu privire la Programul naюional de securitate ciberneticr a Republicii Moldova pentru anii 2016-2020 *//Monitorul Oficial 306-310/905, 13.11.2015*