П О С Т А Н О В Л Е Н И Е

Парламентской Ассамблеи
Организации Договора о коллективной безопасности

О проекте Концепции
плана действий и инструментария в вопросах противодействия
кибервызовам и угрозам

Парламентская Ассамблея Организации Договора о коллективной безопасности п о с т а н о в л я е т:

1. Принять Концепцию плана действий и инструментария в вопросах противодействия кибервызовам и угрозам (далее – Концепция) (прилагается).

2. Направить указанную в пункте 1 настоящего постановления Концепцию в парламенты государств – членов ОДКБ для использования в работе по совершенствованию законодательства государств – членов Организации в соответствующей сфере.

3. Разместить Концепцию на официальном сайте и опубликовать в электронном сборнике материалов Парламентской Ассамблеи ОДКБ.

Председатель
Парламентской Ассамблеи ОДКБ **В.В.ВОЛОДИН**

Москва
30 ноября 2020 года
№ 13-5.4

Приложение
к постановлению ПА ОДКБ
от 30 ноября 2020 года № 13-5.4

Концепция плана действий и инструментария в вопросах противодействия кибервызовам и угрозам

Методология

С целью разработки проекта Концепции плана действий и инструментария в вопросах противодействия кибервызовам и угрозам был составлен план действий, который подразумевает следующие основные шаги:

1. Изучение нормативно-правовой базы всех государств – членов ОДКБ, касающейся вопросов информационной безопасности, кибербезопасности и иных сфер, прямо или косвенно связанных с исследуемыми вопросами. Под нормативно-правовой базой в данном случае подразумеваются как национальное законодательство, так и международные конвенции, которые были подписаны и приравнены к законам. Рассматриваются также национальные стратегии, концепции и доктрины.

2. Инвентаризация имеющихся документов, действующих регуляторов. Составляются списки имеющихся правовых актов и осуществляется их классификация с целью выявления разницы подходов государств-членов к вопросам кибербезопасности и их правовому регулированию.

3. Проведение интервью с ведущими экспертами в сфере кибербезопасности в каждом из государств-членов с целью получения общих оценок существующей правовой базы, определения ее основных недостатков и необходимых механизмов. Интервью, с одной стороны, помогут дополнить инвентаризацию, минимизировать допущения, связанные с недоступностью законодательства на русском языке, с другой стороны, дадут возможность выявить существующие в обществе настроения, составить общее впечатление об имеющемся национальном дискурсе по вопросам кибербезопасности.

4. Содержательное изучение составленной базы, сопоставление ситуации в странах ОДКБ, обобщение вызовов и угроз и необходимых мер. На данном этапе необходимо выделить основные вызовы, общие для всего пространства ОДКБ, а также

общие подходы, не противоречащие национальным законодательствам и дополняющие их.

5. Изучение международного опыта нормативно-правового регулирования вопросов кибербезопасности. Рассматриваются директивы ЕС, а также, по мере необходимости, законы отдельных стран ЕС, чей опыт считается передовым. Возможно также проведение интервью с западными экспертами по кибербезопасности относительно современных глобальных вызовов и мер по противодействию им.

6. Подведение итогов исследования и составление текста проекта.

При изучении национального законодательства и нормативно-правовой базы государств – членов ОДКБ могут быть рассмотрены лишь те документы, которые доступны на русском языке. Исключение составляет Республика Армения, так как разработчики проекта владеют национальным языком и имеют возможность ознакомиться со всей доступной базой.

Вышеупомянутые действия были разделены на несколько этапов.

Итоги первого этапа

На первом этапе были изучены нормативно-правовые базы Российской Федерации и Республики Армения. Составлен список основных актов, регулирующих сферу кибербезопасности, осуществлены классификация выделенных актов и их содержательное исследование. Также изучены некоторые научные публикации с целью дополнения исследования. Проведены интервью с экспертами из Армении и России.

Российская Федерация

В Российской Федерации среди основных документов, определяющих на сегодняшний день фундаментальные подходы к обеспечению информационной безопасности, можно выделить в первую очередь следующие:

1. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года;

3. Концепция внешней политики Российской Федерации;

4. Доктрина информационной безопасности Российской Федерации;

5. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы;

6. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации.

Из современных правовых документов в области безопасности киберпространства выделены следующие:

1. Концепция стратегии кибербезопасности Российской Федерации;

2. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве;

3. Проект Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

4. Указ Президента Российской Федерации от 15 января 2013 года № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

5. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

6. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации;

7. Федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 2 декабря 2019 года) «Об информации, информационных технологиях и о защите информации»;

8. Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

9. Указ Президента Российской Федерации от 22 декабря 2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

10. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

11. Федеральный закон от 26 июля 2017 года № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"»;

12. Федеральный закон от 26 июля 2017 года № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"».

Также рассматриваются:

– Государственная программа «Информационное общество»;

– Конвенция об обеспечении международной информационной безопасности (концепция).

Важно отметить, что как в Российской Федерации, так и в Республике Армения нет единого категориального аппарата в сфере кибербезопасности. В законодательных актах вопросы кибербезопасности охватываются такими вопросами, как защита информации, секретность информации, информационная безопасность и т. д.

В Конституции Российской Федерации защита персональных данных не имела непосредственного закрепления. Вместе с тем под влиянием международно-правовых норм данный вопрос получил развитие в законодательстве.

Базовым документом по информационной безопасности в России является утвержденная Президентом Доктрина информационной безопасности Российской Федерации, которая представляет собой систему официальных взглядов на

обеспечение национальной безопасности Российской Федерации в информационной сфере.

В Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Доктрина информационной безопасности выстраивается на основе определения и защиты национальных интересов Российской Федерации в информационной сфере, среди которых выделяются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации в мирное время, в период непосредственной угрозы, агрессии и в военное время;

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

г) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной

позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

д) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

В соответствии с этими интересами и определяются основные информационные угрозы:

– использование трансграничного оборота информации для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности;

– наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях, осуществление технической разведки в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;

– использование средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств;

– использование со стороны террористических и экстремистских организаций механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников;

– увеличение масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, рост числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны при обработке персональных данных с использованием информационных технологий;

– увеличение масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности;

– постоянное повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усиление разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастание угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации;

– высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран;

– недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий, низкий уровень внедрения отечественных разработок и недостаточное кадровое обеспечение в области информационной безопасности, а также низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности;

– стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

Выделяются четыре основных направления обеспечения информационной безопасности, для каждого из которых определяются основные направления деятельности:

1) сфера государственной и общественной безопасности;
2) экономическая сфера;
3) сфера науки, технологий и образования;
4) сфера стратегической стабильности и равноправного стратегического партнерства.

Основополагающим нормативным правовым актом, регулирующим общественные отношения, связанные с обработкой и защитой персональных данных, является Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», в соответствии с которым такими данными является «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу».

Правовой режим информации в России определяется Федеральным законом «Об информации, информационных технологиях и о защите информации» (от 27 июля 2006 года № 149-ФЗ).

Данным законом (статья 5) информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается[1].

---

[1] Федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 2 декабря 2019 года) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 13 декабря 2019 года).

Обратимся к содержанию некоторых нормативных актов, принятых в течение последних трех лет, что позволит выявить тенденцию развития российского законодательства в этой сфере.

Указ Президента Российской Федерации от 9 мая 2017 года № 203
«О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»

Одним из основных принципов данной Стратегии является обеспечение государственной защиты интересов российских граждан в информационной сфере. В Стратегии закреплены 17 новых информационных понятий, среди которых: индустриальный интернет, интернет вещей, информационное общество, облачные вычисления, туманные вычисления, цифровая экономика, экосистема цифровой экономики.

В Стратегии обращено внимание на то, что с использованием Интернета все чаще совершаются компьютерные атаки на государственные и частные информационные ресурсы и на объекты критической информационной инфраструктуры.

Указ Президента Российской Федерации от 13 мая 2017 года № 208
«О Стратегии экономической безопасности Российской Федерации на период до 2030 года»

В данном правовом акте закреплено, что к основным вызовам и угрозам экономической безопасности Российской Федерации относится стремление развитых государств использовать свои преимущества в уровне развития экономики, высоких технологий (в том числе информационных) в качестве инструмента глобальной конкуренции. Обращено внимание на то, что в настоящее время в России наблюдается слабая инновационная активность, существует отставание в области разработки и внедрения новых и перспективных технологий (в том числе технологий цифровой экономики), недостаточный уровень квалификации и ключевых компетенций отечественных специалистов.

Стратегия также фиксирует основные направления государственной политики в сфере обеспечения экономической безопасности, к которым, в частности, относит создание экономических условий для разработки и внедрения современных

технологий, стимулирование инновационного развития, а также совершенствование нормативно-правовой базы в этой сфере.

Федеральный закон от 1 июля 2017 года № 156-ФЗ

«О внесении изменений в Федеральный закон "Об информации,

информационных технологиях и о защите информации"»

Данным федеральным законом регламентирован новый порядок ограничения доступа к сайту в информационно-телекоммуникационных сетях (в том числе в сети «Интернет»), сходному до степени смешения с сайтом в сети «Интернет», доступ к которому ограничен по решению суда в связи с неоднократным и неправомерным размещением информации, содержащей объекты авторских и (или) смежных прав (копия заблокированного сайта).

Нормы закона, в частности, предусматривают принятие Минкомсвязью России по поступающей информации мотивированного решения о признании сайта в сети «Интернет» копией заблокированного сайта и направление данного решения владельцу такого сайта и в Роскомнадзор для принятия мер по внесудебному ограничению доступа к копии заблокированного сайта.

Федеральный закон от 26 июля 2017 года № 187-ФЗ

«О безопасности критической информационной инфраструктуры

Российской Федерации»

Законом устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры (КИИ), полномочия государственных органов в области обеспечения безопасности КИИ. Определяются также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами КИИ, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

Структурой, контролирующей безопасность КИИ, становится Национальный координационный центр по компьютерным инцидентам.

Собственниками или лицами, пользующимися объектами КИИ на праве аренды или ином законном основании, должны быть российские юридические лица или индивидуальные предприниматели. Указано, что иностранные компании, если они

представляют свои интересы на территории России через российские юридические лица, смогут продолжить свою работу без ограничений.

Законом вводится реестр значимых объектов КИИ, а также устанавливаются требования по обеспечению безопасности значимых объектов КИИ с учетом их категорий. Создаются системы безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования. Безопасность КИИ будет обеспечиваться, в частности, за счет взаимодействия этих систем с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, созданной в соответствии с Указом Президента Российской Федерации от 15 января 2013 года № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Постановление Правительства Российской Федерации от 19 августа 2017 года № 983 «О представлении Президенту Российской Федерации предложения о подписании Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» и Распоряжение Президента Российской Федерации от 26 августа 2017 года № 297-рп «О подписании Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий»

В данных нормативных актах предлагается проект Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий и закрепляется целесообразность его скорейшего подписания на высшем уровне.

Россия присоединилась также к Соглашению о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности.

Конвенцию Совета Европы о киберпреступности Россия не ратифицировала.

Постоянно происходит активное переформатирование существующей и создание новой правовой основы использования информационных технологий в различных сферах жизни общества и функционирования государства. Формируются институты, обеспечивающие реализацию основных направлений государственной политики по противодействию преступлениям в сфере информационных технологий.

В целом законодательство России в сфере информационной безопасности развивается по следующим направлениям:

- закрепление общих положений о доступе к информации, о конфиденциальности и защите информации. Базовым актом здесь является Федеральный закон «Об информации, информационных технологиях и о защите информации»;
- определение правового режима отдельных видов информации:
  - персональных данных – Федеральный закон «О персональных данных»;
  - семейной тайны и тайны личной жизни – Гражданский и Семейный кодексы Российской Федерации;
  - государственной тайны – Закон Российской Федерации «О государственной тайне»;
  - коммерческой тайны – Гражданский кодекс Российской Федерации и Федеральный закон «О коммерческой тайне»;
  - профессиональных, процессуальных тайн – процессуальные кодексы и законы о соответствующих видах деятельности (об адвокатуре, нотариате, охране здоровья граждан и т. п.);
- административное регулирование деятельности по защите информации, в частности связанной с оборотом криптографических средств;
- определение порядка осуществления оперативно-разыскных мероприятий в информационной сфере;
- борьба с преступлениями в сфере информационной безопасности путем закрепления соответствующих составов преступлений в Уголовном кодексе Российской Федерации.

В Уголовном кодексе Российской Федерации содержатся следующие составы преступлений, которые можно отнести к киберпреступности:

▪ неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации (под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи);

▪ создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

▪ нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб;

▪ мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей;

▪ мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации;

▪ изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты, а также электронных

средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

Предварительное следствие и дознание по указанным преступлениям производятся следователями и дознавателями органов внутренних дел Российской Федерации.

Постоянное развитие законодательной базы Российской Федерации позволяет повышать уровень кибербезопасности. Россия – первая по уровню кибербезопасности в регионе СНГ согласно Глобальному индексу кибербезопасности (Global Cyber Security Index) 2018 года и 26-я в глобальном рейтинге[2]. В докладе Международного союза электросвязи (ITU), составляющего ежегодный глобальный индекс кибербезопасности, отмечается, что Российская Федерация имеет самые высокие показатели практически по всем компонентам, кроме уровня сотрудничества; Российская Федерация занимает первое место по показателям в правовом поле и усилила показатели по регулированию предотвращения мошенничества с использованием систем электронных платежей и борьбу с ним; вся финансовая система страны была улучшена с целью укрепления доверия в сфере электронных платежей.

Вместе с тем киберпреступность остается одной из актуальных проблем современной Российской Федерации. Исходя из официальной статистики МВД России за январь – ноябрь 2018 года с использованием компьютерных и информационно-телекоммуникационных технологий было совершено 156 307 преступлений, а за аналогичный период 2017 года – 824 401[3].

На основе анализа современного состояния информационно-телекоммуникационного пространства, научной литературы, аналитических сведений о состоянии преступности и технической оснащенности правоохранительных органов экспертами выделяется ряд проблем, которые требуют скорейшего решения[4]:

---

[2] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[3] Официальный сайт Министерства внутренних дел Российской Федерации, http://mvd.ru/presscenter/statistics/reports/item/804701

[4] Дерюгин Р.А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2 (22).

– деятельность по раскрытию и расследованию преступлений основана на принципах, некоторые из которых уже неэффективны. В настоящее время правоохранительные органы с имеющимся арсеналом технических средств и технологий не всегда могут противостоять «новой преступности» с новейшими технологиями и способами совершения преступлений;

– до конца не урегулирована система государственных учреждений, проводящих компьютерно-технические и иные судебные экспертизы по делам о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий;

– не сформированы предмет, методы, цели и задачи цифровой криминалистики. Это новое перспективное направление требует осмысления и развития ввиду необходимости разработки практических рекомендаций по работе с электронными, виртуальными, цифровыми следами, компьютерной техникой, интернет-сервисами, приложениями и программным обеспечением. Современный правоохранитель обязан владеть такими навыками;

– в сфере кибербезопасности отсутствует эффективное взаимодействие органов внутренних дел с государством, обществом и учреждениями. Меры по противодействию киберугрозам остаются на декларативном уровне, не получая усовершенствования и усиления. Так, до настоящего времени нет сформированной системы оперативного обмена информацией с банковскими организациями, финансово-кредитными учреждениями и даже с операторами сотовой связи. Сведения необходимо получать путем длительных процедур согласования, направления запросов, писем в службу безопасности, проведения судебного санкционирования следственных действий. Перечисленное влияет на оперативность раскрытия преступлений, усложняет процесс расследования, позволяя преступникам тщательно скрывать следы противоправных действий.

Отмечается ряд недостатков правового регулирования постоянно развивающейся сферы киберпреступлений. С развитием информационно-телекоммуникационных технологий будут появляться новые способы совершения преступлений и методы противодействия правоохранительным органам. Современные условия жизни заставляют бороться с анонимными и

неконтролируемыми сервисами, использованием приложений-мессенджеров в преступных целях, «серыми» сим-картами. Эта сфера тоже будет нуждаться в правовом регулировании.

Специалисты Сбербанка выделили топ-5 угроз кибербезопасности на 2019 год. В этот список эксперты банка включили[5]:

- распространение смартфонов, «интернета вещей» и искусственного интеллекта, что может быть использовано злоумышленниками для расширения собственных возможностей;
- распространение концепции BYOD (Bring Your Own Device), согласно которой сотрудники компаний приносят на работу личные ноутбуки и другие устройства;
- развитие высокоскоростных мобильных сетей 5-го поколения (5G), в которых атаки могут стать более массовыми;
- оснащение бытовых приборов различными технологиями для взаимодействия между собой или с внешней средой («интернет вещей»), что увеличивает возможности использования всех этих устройств и образуемых ими сетей в качестве плацдарма для хакерских атак;
- фишинг, или рассылка фейковых сообщений от имени известных фирм, с чем связано более 60% атак на банковский сектор России и многих европейских стран.

Эксперты прогнозируют также основные угрозы на 2020 год. В их число вошли[6]:

– использование искусственного интеллекта, машинного обучения, нейросистем в целях нанесения вреда. Вероятность использования каким-либо мутирующим вирусом машинного обучения, множественных алгоритмов и т. п. очень высокая. Подобные системы опасны тем, что не обнаруживаются большинством традиционных инструментов, поскольку сигнатура «мутантов» постоянно изменяется. Эксперты оценивают частоту появления новых экземпляров

---

[5] https://www.rbc.ru/technology_and_media/15/05/2019/5cdc07689a79470c3d886e6f

[6] Кибербезопасность и угрозы 2020 года: что нас ждет после праздников, https://habr.com/ru/company/zyxel/blog/483976/

ransomware (тип зловредного программного обеспечения, предназначен для вымогательства) в 14 секунд;

– атаки на государственные сети. Возможность атаки на небольшие государственные организации со слабой киберзащитой, обладающие ценными данными, выход в государственные реестры, базы данных и т. п.;

– введение в эксплуатацию сетей пятого поколения (5G). Согласно Research and Markets, до 2025 года объем рынка 5G-решений вырастет в три раза. Среди основных проблем 5G – слабая защищенность компьютеров, разного рода опасности в цикле «производство – поставка – внедрение». В некоторых случаях преступники внедряют уязвимость в продукты сторонних производителей, предприятия или организации;

– увеличение количества атак на облачные сервисы. Целью атак могут стать сервисы хранения данных, мессенджеры, социальные сети. Например, атаки на Microsoft OneDrive, Google Drive и другие сервисы хранения данных;

– распространение медицинских устройств, работающих с беспроводными сетями.

К основным недостаткам законодательства Российской Федерации в сфере информационной безопасности относят следующие[7]:

1. Несогласованность между информационно-коммуникационными технологиями (большие данные, облачные технологии, суперкомпьютеры, искусственный интеллект и т. д.) и законодательством Российской Федерации, регулирующим вопросы безопасности в этой сфере, развития и использования цифровых технологий. Например, не упорядочена и не введена в правовое поле сфера сбора в Интернете личных данных граждан и их использования.

2. Неоднозначность положений некоторых законов, которые по-разному трактуются государственными регуляторами и операторами, требуют конкретизации, уточнений и разъяснений.

3. Неоднозначность терминологии.

---

[7] Информационный суверенитет или почему России нужна стратегия информационной безопасности, РСМД, https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-suverenitet-ili-pochemu-rossii-nuzhna-strategiya-informatsionnoy-bezopasnosti/

4. Необходимость адаптации законодательства государства к глобальным угрозам информационной безопасности на международном уровне. В частности, разработка и принятие Стратегии информационной безопасности России, гармонизация и унификация законодательства государств-союзников и партнеров Российской Федерации в условиях формирования глобального информационного пространства и ускоренного роста глобальных угроз информационной безопасности; совершенствование законодательства Российской Федерации, способствующего созданию международной нормативно-правовой базы по борьбе с ИКТ-угрозами.

Также среди основных проблем отмечаются:

1) сложность и дороговизна системы технической защиты информационных систем персональных данных;
2) зависимость информационной безопасности Российской Федерации от иностранных поставщиков программно-аппаратных компонентов программного обеспечения и оборудования (браузеры, поисковики, социальные сети, операционные системы находятся вне пределов российского контроля);
3) нехватка квалифицированных специалистов, программного обеспечения и недостаточность координации с правоохранительными органами;
4) несовершенство информационной безопасности в социальной и образовательной сферах и т. д.

Обзор российского законодательства в сфере кибербезопасности и составление списка основных угроз будут дополнены, в частности по результатам проведения интервью с экспертами.

Республика Армения

В Республике Армения государственная политика в сфере информационной безопасности и кибербезопасности регулируется следующими актами:

1. Закон Республики Армения «О полиции»;
2. Закон Республики Армения «Об органах национальной безопасности»;
3. Уголовный кодекс Республики Армения;
4. Конвенция Совета Европы о киберпреступности;

5. Закон Республики Армения «Об обороне»;

6. Концепция информационной безопасности Республики Армения;

7. Концепция формирования электронного общества;

8. Национальная программа борьбы с организованной преступностью;

9. Национальная стратегия борьбы с терроризмом;

10. Стратегическая программа электронного управления;

11. Программа правительства от 2017 года.

Вопросы кибербезопасности особенно актуальны для Армении в связи с наличием нагорно-карабахского конфликта и его трансформацией, в частности, в информационную войну на пространстве Интернета. Армения нередко становится мишенью для азербайджанских и турецких хакерских групп, при этом уровень кибербезопасности Армении довольно низкий. Одна из основных проблем – отсутствие необходимых регуляторов правового поля в сфере кибербезопасности.

Конституционно-правовые нормы о защите персональных данных закреплены в Конституции Республики Армения (статья 34).

В настоящее время разрабатывается новая Стратегия национальной безопасности Республики Армения. В действующей Стратегии национальной безопасности (одобрена на заседании Совета национальной безопасности при Президенте Республики Армения 26 января 2007 года) отмечается, что Республика Армения придает важность:

– интеграции в международное информационное пространство;

– профессиональному формированию у международного сообщества истинных представлений об Армении и армянстве, противодействию дезинформации и негативной пропаганде;

– обеспечению сбалансированной по объему и качеству необходимой информации на армянском языке в глобальной сети «Интернет», посвященной Армении, по отраслям арменоведения и связанным с армянством вопросам.

Первую Концепцию информационной безопасности Республики Армения, принятую в 2009 году, заменила в 2017 году Концепция информационной безопасности и информационной политики Республики Армения, которая, однако, не была

опубликована. Сейчас, согласно заявлениям секретаря Совета безопасности Республики Армения А. Григоряна, на стадии разработки находится новый проект Концепции кибербезопасности Армении.

Для составления общего впечатления о государственном подходе к определению киберугроз обратимся к некоторым основным пунктам Концепции от 2009 года.

Так, в указанной Концепции в качестве национальных интересов Армении в сфере информационной безопасности выделялись:

- минимизация негативного влияния угроз национальным интересам Республики Армения в информационном пространстве, проактивность в процессе защиты национальных и государственных целей, обеспечение информационной безопасности Республики Армения как во внутреннем, так и на международном информационном пространстве;
- информационная безопасность Республики Армения – защита национальных интересов Республики Армения в информационной сфере с учетом взаимосвязи интересов личности, общества и государства.

Среди основных составляющих национальных интересов отмечаются следующие:

1. Защита конституционных прав и свобод человека и гражданина в области получения и использования информации, обеспечение духовного развития страны, сохранение и укрепление нравственных ценностей общества, патриотических и гуманитарных традиций, культурного и научного потенциала.

2. Обеспечение информационной политики Республики Армения, связанной с предоставлением достоверной информации об Армении армянскому обществу и международному сообществу, с информированием об официальной государственной позиции по важнейшим политическим и социальным событиям в жизни государства и мира с одновременным обеспечением доступности открытой информации для граждан.

3. Развитие современных информационных технологий для удовлетворения внутреннего спроса и экспорта на мировой рынок, а также накопление, сохранение и эффективное использование носителей информации.

4. Вовлечение информационного сектора страны в международное информационное поле, беспристрастное и профессиональное представление международному сообществу правдивой информации об Армении и армянах, противодействие дезинформации и ложной пропаганде, обеспечение необходимого объема и качества информации, связанной с армянским языком и Арменией, арменоведением и армянством в Интернете.

5. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных, коммуникационных и телекоммуникационных систем.

Еще в 2017 году по поручению Президента Армении С. Саргсяна был разработан проект решения Правительства о принятии стратегии кибербезопасности, которой был опубликован, но не утвержден.

Документ был разработан Министерством высокотехнологичной промышленности. Согласно проекту, разработка стратегии кибербезопасности была продиктована необходимостью обеспечения безопасной и надежной деятельности инфраструктур в физических и виртуальных пространствах. В документе отмечалось, что деятельность физических инфраструктур по большей части зависит от надежности цифровых инфраструктур, а также критических информационных инфраструктур. Следовательно, сбои в их работе могут нанести существенный урон государству.

Примечательно, что согласно этому документу предполагалось наладить сотрудничество между государственным и частным секторами, в частности для обеспечения безопасности банковских, общественных и телекоммуникационных услуг. Предусматривалось создание Центра кибербезопасности, который был бы отдельным органом и занимался бы разработкой политики кибербезопасности, аудитом, обеспечением взаимосвязи между государственными органами и профессиональным консультированием, изучением международного опыта и проведением обучающих программ.

Главным препятствием для принятия стратегии стало отсутствие единых подходов.

В Республике Армения отсутствует также закон о критической инфраструктуре, нет цельного регулирования этой сферы.

Согласно исследованию портала ampop.am, армянская государственная политика кибербезопасности не предполагает обеспечение кибербезопасности для таких важных инфраструктур страны, как системы электричества, питьевой воды, аэропорта, ядерной промышленности. Из-за отсутствия надлежащего аудита в этих инфраструктурах невозможно выяснить, по каким системам работают данные службы и каков их уровень защиты от киберугроз.

В вопросе управления киберсферой Армении отсутствует систематизированный подход. Отдельные ведомства самостоятельно пытаются обеспечить свою безопасность, нет всеобщей, единой или общегосударственной системы.

В международных докладах также отмечается, что причиной неутешительных результатов Армении по обеспечению кибербезопасности являются проблемы с организацией, развитием навыков и возможностей, а также с сотрудничеством.

В программе Правительства от 2019 года вопросы информационной безопасности отражены в разделе «Связь и цифровое вещание». Отмечается, что Правительство собирается осуществлять:

– шаги, направленные на внедрение цифровых технологий во всех отраслях экономики Республики Армения, обеспечивая информационную безопасность, кибербезопасность и защиту персональных данных;

–разработку государственных стандартов обеспечения информационной безопасности, их внедрение и контроль.

Подробности, касающиеся защиты персональных данных, определяются Законом Республики Армения «О защите персональных данных» (принят 18 мая 2015 года). Закон, в частности, регулирует порядок и условия обработки персональных данных органами государственного управления и местного самоуправления, государственными и муниципальными учреждениями, организациями, юридическими и физическими лицами, а также сроки и условия осуществления государственного контроля над ними.

Законом допускается регулирование иными актами особенностей обработки персональных данных, используемых:

- в государственной и служебной деятельности;
- в банковской деятельности;
- в нотариальной деятельности;
- в адвокатской деятельности;
- в процессе деятельности, связанной с конфиденциальностью страхования;
- в процессе деятельности, связанной с национальной безопасностью или обороной;
- в процессе борьбы с отмыванием денег и терроризмом;
- в процессе оперативно-разведывательной деятельности;
- в судебных процессах.

Ограничения обработки персональных данных, предусмотренные Законом, не распространяются на обработку персональных данных в журналистских, художественных или литературных целях.

Некоторые вопросы защиты персональных данных регулируются также:

– статьей 25 Закона Республики Армения «Об адвокатуре» (2004 года);

– статьей 5 Закона Республики Армения «О нотариате» (2001 года);

– Законом Республики Армения «О банковской тайне» (1996 года);

– статьей 5 Закона Республики Армения «О борьбе с отмыванием денег и финансированием терроризма» (2008 года) и др.

В Уголовном кодексе Республики Армения уголовные наказания за правонарушения в сфере защиты секретной информации относятся к следующим действиям:

– незаконный сбор, хранение, использование или распространение информации о личной или семейной жизни (статья 144);

– нарушение конфиденциальности переписки, телефонных разговоров, почты, телеграмм или других сообщений (статья 146);

– незаконный сбор или публикация коммерческой, страховой или банковской секретной информации (статья 199);

– раскрытие медицинских секретов (статья 145).

Согласно статье 189.17 Кодекса Республики Армения об административных правонарушениях за нарушение Закона «О защите персональных данных» предусмотрена административная ответственность.

Попытки регулирования информационной безопасности в банковской сфере осуществляются Центральным банком Республики Армения. 9 июля 2013 года было опубликовано Рекомендательное решение Центрального банка об утверждении порядка установления минимальных требований по обеспечению информационной безопасности. В документе отмечается, что все банки, операторы регулируемого рынка, центральный депозитарий, кредитные бюро и другие организации, действующие в этой сфере, обязаны привести свою систему информационной безопасности в соответствие с действующими в этой сфере международными стандартами и получить соответствующие сертификаты.

Армения присоединилась также к Соглашению о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности, к Соглашению о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности и к Конвенции Совета Европы о киберпреступности.

Концепция формирования электронного общества была принята в Армении на 2010–2012 годы. Концепция предусматривала ряд шагов, направленных на обеспечение электронной безопасности, в том числе принятие законов, регулирующих сферу электронных отношений, которые должны соответствовать принципам кибербезопасности.

В принятой в 2012 году в Армении Национальной стратегии борьбы с терроризмом особое внимание уделяется информационной безопасности и борьбе с киберпреступностью. В документе детально рассматриваются основные угрозы кибертерроризма, цели и задачи борьбы с ним и необходимые шаги в этом направлении. Большое значение придается подготовке специализированных кадров, развитию правовой базы, формированию единой государственной политики и т. д.

Вопросами кибербезопасности государственных ведомств – министерств, Центробанка, комитетов и прочих – занимается Служба национальной безопасности

Республики Армения (СНБ). При этом в Армении отсутствует единый свод законов по кибербезопасности, систематизирующий угрозы и риски, общие подходы и критерии экстренного реагирования.

Законодательство в целом не отражает современные реалии ИТ-сферы. Как таковые отсутствуют ответственные общественные или отраслевые органы кибербезопасности. В ряде структур, например в СНБ, существуют соответствующие отделы, которые решают вопросы защиты крайне ограниченных пространств. Отсутствие четкой стратегии приводит к отсутствию стандартов. В то же время Армения выступает активным актором в сотрудничестве на международном уровне.

Согласно Глобальному индексу кибербезопасности (Global Cyber Security Index) на 2018 год Армения занимает 79-е место в глобальном рейтинге и 6-е место среди стран СНГ.

Эксперты отмечают ряд факторов, способствующих уязвимости киберпространства Армении:

1) бурное развитие телекоммуникационной сферы, ведущее к более глубокому проникновению в киберпространство инфраструктур страны, что, в свою очередь, создает множество новых уязвимых узлов;

2) развитие кибератакующих сил Азербайджана, DDoS-атаки на государственные и информационные сетевые сегменты Армении;

3) уязвимость критически важных узлов Армении для третьих сторон;

4) отсутствие оценки уязвимых узлов Армении и их защитных возможностей;

5) недостаточная информированность общества.

Есть предложения по созданию общественного органа кибербезопасности, который будет содействовать негосударственным структурам, информировать общественность о существующих киберугрозах, оказывать поддержку в борьбе с киберпреступностью негосударственным критическим узлам – банковской, энергетической сферам, сфере общественных услуг и пр.

К основным вызовам кибербезопасности Армении эксперт по вопросам цифровой безопасности и новых медиа С.Мартиросян[8] относит:

– отсутствие Стратегии кибербезопасности;

– отсутствие единого государственного или национального органа, который мог бы курировать и регулировать в целом вопросы кибербезопасности (сегодня основные вопросы, связанные с кибербезопасностью, регулируются просто посредством экстраполяции офлайна на онлайн);

– отсутствие понимания критических инфраструктур и их защиты;

– отсутствие элементов кибербезопасности в образовательной системе, как школьной, так и вузовской;

– отсутствие стандартов по обеспечению информационной безопасности.

Единственный стандарт, который в принудительном порядке работает только в банковской сфере, это ISO/IEC 27001, но он слишком высокий. Для среднего и малого бизнеса стандартов нет, и, соответственно, не ясно, как это должно регулироваться.

Обзор армянского законодательства в сфере кибербезопасности с составлением списка основных угроз будет дополнен по результатам проведения интервью с другими экспертами.

Выше изложены итоги работы, проделанной в рамках первого этапа. В дальнейшем предполагается закончить инвентаризацию правовой базы Российской Федерации и Республики Армения, основываясь, в частности, на результатах интервью с экспертами.

При исследовании законодательных основ и анализе законодательства государств – членов ОДКБ в сфере нормативно-правового регулирования противодействия кибервызовам и угрозам особое внимание уделяется следующим существующим угрозам:

1) вымогательство путем использования незаконного доступа к компьютерам, мобильным устройствам, аккаунтам в социальных сетях и кабинетам на общедоступны сайтах и т. д.;

---

[8] Интервью проведено в рамках исследования.

2) хулиганство, распространение материалов незаконного характера, подстрекательство, пропаганда насилия, терроризма и призывы к насильственным действиям;

3) распространение наркотических средств, формул синтетических наркотиков (спайсов) и другой информации по изготовлению различных наркотиков;

4) мошенничество, обманные операции с движимым и недвижимым имуществом, драгоценными металлами и камнями, антиквариатом и т. д.;

5) финансовые пирамиды, отмывание денежных средств, незаконные азартные игры, ложные лотереи, подставные или нереальные брокерские махинации, продажа несуществующих на реальном рынке ценных бумаг и т. д.;

6) фальшивые аукционы, не существующие в реальной жизни интернет-магазины, ложные благотворительные акции;

7) преследование, незаконный сбор персональных данных и их использование, идентификация лиц;

8) незаконное прослушивание голосовых переговоров или отслеживание и просмотр переписок, а также фото- и видеоматериалов;

9) предложение незаконных или нереальных услуг мошеннического характера;

10) международная, военная, промышленная, деловая, политическая шпионская деятельность;

11) распространение вирусов (вредоносных программ) с целью вредительства либо в рамках одного или нескольких вышеперечисленных пунктов.

Поскольку при реализации почти всех перечисленных преступлений или незаконных действий злоумышленники в общей цепи событий частично или полностью действуют в интернет-пространстве, то нередко их действия выходят за рамки уголовного права, регулирующего ответственность за преступления в реальной жизни, по причине отсутствия законов, относящихся к конкретным действиям в Интернете или с использованием Интернета.

Итоги второго этапа

Республика Беларусь

В Республике Беларусь государственная политика в сфере информационной безопасности и кибербезопасности регулируется следующими актами:

- Концепция национальной безопасности Республики Беларусь;
- Концепция информационной безопасности Республики Беларусь;
- Уголовный кодекс Республики Беларусь;
- Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы;
- Закон Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации»;
- Кодекс Республики Беларусь об административных правонарушениях, в частности глава 22 «Административные правонарушения в области связи и информации»;
- Декрет Президента Республики Беларусь от 21 декабря 2017 года № 8 «О развитии цифровой экономики»;
- Указ Президента Республики Беларусь от 16 апреля 2013 года № 196 «О некоторых мерах по совершенствованию защиты информации»;
- Указ Президента Республики Беларусь от 1 февраля 2010 года № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»;
- Закон Республики Беларусь от 28 декабря 2009 года № 113-З «Об электронном документе и электронной цифровой подписи»;
- проект Закона Республики Беларусь «О защите персональных данных» и т. д.

К базовым нормотворческим документам также относятся:

- Государственная программа развития цифровой экономики и информационного общества на 2016–2020 годы;

- Стратегия Республики Беларусь в сфере интеллектуальной собственности на 2012–2020 годы;
- Стратегия «Наука и технологии: 2018–2040».

Беларусь – пятая по уровню кибербезопасности в регионе СНГ согласно Глобальному индексу кибербезопасности (Global Cyber Security Index) на 2018 год и 69-я в глобальном рейтинге[9].

В Конституции Республики Беларусь защита персональных данных не получила непосредственного закрепления.

Вопросы информационной безопасности закреплены в Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 года № 575.

Информационная безопасность в Концепции определяется как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Кибербезопасность определяется как состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Выделяются следующие основные интересы в информационной сфере:

- реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
- формирование и поступательное развитие информационного общества;
- равноправное участие Республики Беларусь в мировых информационных отношениях;
- преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
- эффективное информационное обеспечение государственной политики;
- обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

[9] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Среди основных потенциальных либо реально существующих угроз национальной безопасности отмечены следующие угрозы, связанные с информационной безопасностью:

1) деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;
2) нарушение функционирования критически важных объектов информатизации;
3) недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;
4) снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;
5) утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности.

Выделяются следующие внутренние источники угроз национальной безопасности в информационной сфере:

– распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

– зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

– несоответствие качества национального контента мировому уровню;

– недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

– рост преступности с использованием информационно-коммуникационных технологий;

– недостаточная эффективность информационного обеспечения государственной политики;

– несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Выделяются следующие внешние источники угроз национальной безопасности в информационной сфере:

– открытость и уязвимость информационного пространства Республики Беларусь для внешнего воздействия;

– доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;

– информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;

– нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

– развитие технологий манипулирования информацией;

– препятствование распространению национального контента Республики Беларусь за рубежом;

– широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

– попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

В Концепции отмечается, что «в информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии

всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной

политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий».

Среди основных индикаторов состояния национальной безопасности также отмечается уровень развития информационных технологий и телекоммуникаций.

В Концепции информационной безопасности Республики Беларусь, утвержденной 18 марта 2019 года, отмечаются следующие цели и направления государственной политики.

Цель определяется как достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

В соответствии с ней выделены следующие направления государственной политики:

1. Мониторинг, анализ и оценка состояния информационной безопасности. Применяются индикаторы оценки ее состояния. Определяются приоритетные направления предотвращения угроз информационной безопасности, минимизации их деструктивного воздействия и локализации последствий. Разрабатывается и реализуется комплекс мер стратегического и тактического характера по предупреждению и нейтрализации информационных рисков, вызовов и угроз.

2. Обеспечение конституционного права граждан свободно искать, получать, передавать, производить, хранить и распространять информацию любым законным способом, права на тайну личной жизни и иную охраняемую законом тайну,

защиту персональных данных и авторских прав, а также соблюдение баланса прав и ограничений, связанных с обеспечением национальной безопасности.

3. Содействие защищенности национальных информационных систем, обеспечению безопасности используемого гражданами и организациями программного обеспечения. В целях улучшения устойчивости государственного сектора к информационным рискам осваиваются передовые технологии, внедряются новые средства и способы обеспечения информационной безопасности.

4. Разработка стандартов информационной безопасности и с их учетом проведение аудита государственных систем информационной безопасности. Развивается смарт-проектирование решений по обеспечению информационной безопасности. На нормативном уровне выделяется и регламентируется функционирование критически важных объектов информатизации. Поощряется развитие технологий безопасности в бизнесе и жизнедеятельности граждан.

5. Криминализация деяний, причиняющих существенный вред правоохраняемым интересам в информационной сфере или создающих опасность его причинения. Криминализируются в уголовном законе в соответствии с существующими мировыми подходами. Реализуются шаги по снижению угроз киберпреступности, в том числе кибертерроризма, расследованию и пресечению действий вовлеченных в террористическую деятельность лиц, перекрытию каналов пропаганды терроризма, привлечения и вербовки сторонников, поощрения и провоцирования террористической активности, финансирования терроризма.

6. Развитие взаимодействия государства, общественности, бизнес-сообщества, СМИ в целях своевременного обнаружения рисков и вызовов информационной безопасности, воспрепятствования кибератакам и акциям деструктивного информационного воздействия, повышения эффективности правоохранительной деятельности.

7. Уделение особого внимания кадровому потенциалу в обеспечении информационной безопасности. На современном образовательном и технологическом уровне осуществляется специальная подготовка, переподготовка и повышение профессиональной квалификации лиц, обеспечивающих информационную

безопасность, сотрудничество между государственными органами, учреждениями образования и отраслевыми предприятиями в подборе, подготовке и трудоустройстве таких кадров, интегрирование тематики информационной безопасности в образовательные программы всех уровней обучения. Формируется государственный заказ на подготовку кадров.

8. Производство средств обеспечения информационной безопасности. Наращивается научный потенциал и финансирование работ по исследованию и созданию новых решений в сфере обеспечения информационной безопасности, в том числе технической защиты информации, криптологии, криминологии, криминалистики. Государство осуществляет финансирование приоритетных направлений обеспечения информационной безопасности, прежде всего в рамках государственных программ. Разрабатываются инновационные методы и технологии защиты информационных ресурсов и систем.

9. Приложение усилий по повышению действенности международного права и соблюдению моральных норм ответственного поведения в информационном пространстве. Оказывается содействие разработке и внедрению мер по укреплению доверия в информационном пространстве. Создаются и развиваются каналы международного обмена опытом в области обеспечения информационной безопасности, а также информацией об угрозах национальным интересам, в том числе уязвимостях информационных систем, инцидентах в информационной инфраструктуре.

Некоторые преступления, связанные с кибербезопасностью, отражены в Уголовном кодексе Республики Беларусь от 9 июля 1999 года № 275-З. Например: часть 2 статьи 343 («Изготовление и распространение порнографических материалов или предметов порнографического характера»), часть 2 статьи 343^1, статья 212 («Хищение путем использования компьютерной техники»), статья 349 («Несанкционированный доступ к компьютерной информации»), статья 350 («Модификация компьютерной информации»), статья 351 («Компьютерный саботаж»), статья 352 («Неправомерное завладение компьютерной информацией»), статья 353 («Изготовление либо сбыт специальных средств для получения неправомерного

доступа к компьютерной системе или сети»), статья 354 («Разработка, использование либо распространение вредоносных программ»), статья 355 («Нарушение правил эксплуатации компьютерной системы или сети»).

В 2015 году утверждена Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы, которая определяет следующие основные направления обеспечения информационной безопасности:

– организация научных исследований, разработка и производство собственных аппаратных и программных средств защиты информации, ключевых элементов информационно-коммуникационной инфраструктуры, совершенствование системы их стандартизации, сертификации и аттестации в целях создания «цифрового суверенитета» Республики Беларусь;

– совершенствование нормативно-правовой и нормативно-технической базы для доступного, эффективного и беспрепятственного информационного взаимодействия государства, бизнеса и граждан;

– организация хранения персональных данных граждан Республики Беларусь исключительно в центрах обработки данных и дата-центрах на территории Республики Беларусь;

– создание необходимого уровня защиты информации, содержащейся в государственных информационных ресурсах;

– резервирование информационных сетей республиканских органов государственного управления;

– активное использование возможностей белорусского спутника связи и вещания для увеличения информационного присутствия страны в мировом информационном пространстве.

Как правовая категория «информационная безопасность» закреплена только в законах, ратифицирующих международные соглашения с Российской Федерацией и государствами – участниками СНГ в области обеспечения международной информационной безопасности.

Понятие «кибербезопасность» в национальном законодательстве не встречается и не имеет юридического толкования. Впервые оно было зафиксировано лишь в 2019 году в принятой Концепции информационной безопасности Республики Беларусь.

Основной целью Закона «Об информации, информатизации и защите информации» является регулирование отношений, возникающих в процессе жизненного цикла информации, при создании и использовании информационных технологий, систем, сетей, ресурсов, а также при организации и обеспечении защиты информации. Закон устанавливает требования по защите информации, а также ссылается на иные законодательные акты Республики Беларусь, в которых закреплена ответственность за нарушение законодательства об информации, информатизации и защите информации.

Функцию регулятора, контролирующего обеспечение защиты информации от утечки и несанкционированных действий, выполняет Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ). Для противодействия преступлениям в области информационной безопасности в 2001 году в Министерстве внутренних дел Республики Беларусь создано управление по раскрытию преступлений в сфере высоких технологий (УРПСВТ, или управление «К»).

Приоритетными направлениями в развитии обеспечения информационной безопасности эксперты считают совершенствование нормативно-правовой базы, завершение формирования комплексной государственной системы обеспечения информационной безопасности, в частности путем оптимизации механизмов государственного регулирования деятельности в данной сфере. При этом большое значение придается усилению деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством[10].

Среди основных проблем обеспечения информационной безопасности частных и государственных компаний эксперты отмечают использование несертифицированного

---

[10] Полковниченко Ю.В., Чудиловская Т.Г. Правовое регулирование информационных отношений в области информационной безопасности // Теоретические и прикладные проблемы информационной безопасности : материалы Международной научно-практической конференции (Минск, 18 мая 2017 г.). Минск : Академия МВД Республики Беларусь, 2018. С. 59–63.

оборудования и программного обеспечения, несоблюдение правовых, организационных и технических требований.

Республика Казахстан

В Республике Казахстан среди основных документов, определяющих фундаментальные подходы к обеспечению информационной безопасности, можно выделить Концепцию «Киберщит Казахстана» и Стратегию «Казахстан-2050».

Государственная политика в сфере информационной безопасности и кибербезопасности регулируется следующими актами:

- Закон Республики Казахстан «О национальной безопасности Республики Казахстан»;
- Закон Республики Казахстан «Об информатизации»;
- Закон Республики Казахстан «О связи»;
- Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности от 20 декабря 2016 года;
- Государственная программа «Информационный Казахстан – 2020»;
- Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации»;
- Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи».

Республика Казахстан занимает второе место по уровню кибербезопасности в регионе СНГ согласно Глобальному индексу кибербезопасности (Global Cyber Security Index) на 2018 год и 40-е в глобальном рейтинге[11]. В докладе Международного союза электросвязи (ITU), составляющего ежегодный Глобальный индекс кибербезопасности, отмечается, что Казахстан имеет хорошие показатели, занимая второе место практически по всем компонентам, кроме уровня

[11] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

сотрудничества. Особенно положительную оценку получил компонент правового регулирования.

В Конституции Республики Казахстан, принятой в 1995 году и дополненной 23 марта 2019 года, отражено «право на тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений».

Концепция кибербезопасности («Киберщит Казахстана»), утвержденная 30 июня 2017 года, представляет собой доктринальный документ второго поколения: он разработан в соответствии с проблемно-целевым подходом и детально определяет параметры (свойства) безопасности информации. Акцент сделан не на внешние угрозы, а на внутренние проблемы, связанные с общественными отношениями. В Концепции содержатся ожидаемые результаты с четкими статистическими (рейтинговыми) параметрами по каждой из определенных стратегических задач, распределенных между государственными органами, также предполагается этапность достижения заданных показателей безопасности, ресурсное обеспечение и правовое сопровождение.

Под кибербезопасностью в Концепции понимается состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации.

В Концепции выделяются следующие угрозы в сфере кибербезопасности:

- низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности;
- нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере ИКТ установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме;
- непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное

обеспечение и другие элементы информационно-коммуникационной инфраструктуры;

– действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг;

– деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру.

Цель Концепции определяется как достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.

В Концепции сформулированы следующие задачи:

1. Формирование необходимых условий для повышения осведомленности об угрозах, для развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов и систем кибербезопасности, направленных на блокирование и подавление вредоносного программно-технического воздействия и защищенного телекоммуникационного оборудования.

2. Совершенствование правоприменительной практики, методологической базы, нормативно-правового и организационно-технического обеспечения безопасного использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами.

3. Создание высокоадаптивной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно-коммуникационной инфраструктуры.

В Концепции приводится также перечень нормативных правовых актов, посредством которых предполагается ее реализация:

1) Уголовный кодекс Республики Казахстан от 3 июля 2014 года;

2) Кодекс Республики Казахстан «Об административных правонарушениях» от 5 июля 2014 года;

3) Предпринимательский кодекс Республики Казахстан от 29 октября 2015 года;

4) Закон Республики Казахстан от 15 сентября 1994 года «Об оперативно-розыскной деятельности»;

5) Закон Республики Казахстан от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан»;

6) Закон Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи»;

7) Закон Республики Казахстан от 5 июля 2004 года «О связи»;

8) Закон Республики Казахстан от 27 июля 2007 года «Об образовании»;

9) Закон Республики Казахстан от 18 февраля 2011 года «О науке»;

10) Закон Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан»;

11) Закон Республики Казахстан от 21 мая 2013 года «О персональных данных и их защите»;

12) Закон Республики Казахстан от 11 апреля 2014 года «О гражданской защите»;

13) Закон Республики Казахстан от 16 мая 2014 года «О разрешениях и уведомлениях»;

14) Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации»;

15) Закон Республики Казахстан от 4 декабря 2015 года «О государственных закупках»;

16) Государственная программа «Цифровой Казахстан» от 12 декабря 2017 года;

17) Стратегия кибербезопасности финансового сектора Республики Казахстан на 2018–2022 годы;

18) постановление Правительства Республики Казахстан от 9 августа 2018 года «Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности».

Кроме того, в данный перечень вошли указы и другие постановления.

В Стратегии «Казахстан-2050», представленной в декабре 2012 года в Послании главы государства, отмечается, что «государство должно стимулировать развитие транзитного потенциала в сфере информационных технологий. К 2030 году мы должны пропускать через Казахстан не менее 2–3% мировых информационных потоков. К 2050 году эта цифра должна как минимум удвоиться». При этом «сегодня, в век Интернета и высоких технологий, когда информационный поток колоссален, "фильтр" должен быть внутри человека».

Относительно новой политики развития инновационных исследований отмечается: «Нам нужен трансферт необходимых стране технологий и обучение специалистов для их использования. EXPO-2017 должно дать толчок этому процессу и помочь нам отобрать новейшие технологии для развития энергетики будущего».

В соответствии с Законом «О национальной безопасности Республики Казахстан» информационная безопасность обеспечивается решениями и действиями государственных органов, организаций, должностных лиц, направленными на:

1) недопущение информационной зависимости Казахстана;

2) предотвращение информационной экспансии и блокады со стороны других государств, организаций и отдельных лиц;

3) недопущение информационной изоляции Президента, Парламента, Правительства и сил обеспечения национальной безопасности Республики Казахстан;

4) обеспечение бесперебойной и устойчивой эксплуатации сетей связи в целях сохранения безопасности Республики Казахстан, в том числе в особый период и при возникновении чрезвычайных ситуаций природного, техногенного характера, карантинов, иных чрезвычайных ситуаций;

5) выявление, предупреждение и пресечение утечки и утраты сведений, составляющих государственные секреты и иную защищаемую законом тайну;

6) недопущение информационного воздействия на общественное и индивидуальное сознание, связанного с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности;

7) обнаружение и дезорганизацию механизмов скрытого информационного влияния на процесс выработки и принятия государственных решений в ущерб национальной безопасности;

8) поддержание и развитие эффективной системы защиты информационных ресурсов, информационных систем и инфраструктуры связи, в которых циркулируют сведения, составляющие государственную, коммерческую и иную защищаемую законом тайну.

Особое внимание уделяется системе обеспечения информационной безопасности, в том числе государственных электронных информационных ресурсов, информационных систем, информационно-коммуникационной инфраструктуры и критически важных объектов информационно-коммуникационной инфраструктуры.

В 2014 году в Казахстане был принят новый Уголовный кодекс. Одной из особенностей нового уголовного закона стало включение целого ряда составов уголовных правонарушений в сфере информатизации и связи. Предыдущая редакция Уголовного кодекса не содержала аналогичных составов.

Обратимся к основным статьям.

Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций

1. Умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства…

2. То же деяние, совершенное в отношении критически важных объектов информационно-коммуникационной инфраструктуры…

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия…

Статья 206. Неправомерные уничтожение или модификация информации

1. Умышленные неправомерные уничтожение или модификация охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, а равно ввод в информационную систему заведомо ложной информации, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства…

2. Те же деяния, совершенные:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры…

2) группой лиц по предварительному сговору…

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия…

Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций

1. Умышленные действия (бездействие), направленные на нарушение работы информационной системы или сетей телекоммуникации…

2. Те же деяния, совершенные:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору…

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия…

Статья 208. Неправомерное завладение информацией

1. Умышленное неправомерное копирование или иное неправомерное завладение охраняемой законом информацией, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства…

2. То же деяние, совершенное:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору…

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия…

Статья 209. Принуждение к передаче информации

1. Принуждение к передаче охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, под угрозой применения насилия либо уничтожения или повреждения имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может причинить существенный вред интересам потерпевшего или его близких…

2. То же деяние:

1) сопряженное с применением физического насилия над лицом или его близкими;

2) совершенное группой лиц по предварительному сговору;

3) совершенное с целью получения информации из критически важных объектов информационно-коммуникационной инфраструктуры…

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия…

Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов

1. Создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно умышленные использование и (или) распространение такой программы или программного продукта…

2. Те же деяния, совершенные:

1) группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения;

3) в отношении критически важных объектов информационно-коммуникационной инфраструктуры…

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия…

Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа

1. Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем…

2. То же деяние, совершенное:

1) группой лиц по предварительному сговору;

2) из корыстных побуждений;

3) лицом с использованием своего служебного положения…

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия…

Статья 212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели

1. Заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в открытой сети телекоммуникаций для размещения интернет-ресурсов, преследующих противоправные цели…

2. То же деяние, совершенное группой лиц по предварительному сговору или преступной группой…

Статья 213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства

1. Изменение идентификационного кода абонентского устройства сотовой связи, создание дубликата карты идентификации абонента сотовой связи, если эти действия совершены без согласия производителя или законного владельца…

2. Неправомерные создание, использование, распространение программ, позволяющих изменять идентификационный код абонентского устройства сотовой связи или создавать дубликат карты идентификации абонента сотовой связи…

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные преступной группой…

За непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации в центральном аппарате Министерства информации и общественного развития Республики Казахстан отвечает Департамент информационных технологий и государственных услуг.

Ключевым вопросом обеспечения информационной безопасности Республики Казахстан является вопрос контроля за хранением и распространением информации. Информация, распространяемая в сетях телекоммуникации, включает в себя как персональные данные пользователей, так и государственные секреты и другую закрытую информацию. Поэтому так важно иметь достаточную правовую основу для создания стабильной системы в сфере хранения и распространения информации.

Анализ законодательства в сфере хранения и распространения информации выявил ряд проблемных вопросов, которые требуют принятия мер для их последующего решения. Во-первых, сегодня источники информационных угроз могут находиться вне юрисдикции законодательства Республики Казахстан, что существенно затрудняет применение системы правовых мер. Во-вторых, в соответствии с подпунктом 2 пункта 1 статьи 15 Закона Республики Казахстан «О связи» операторы связи и (или) владельцы сетей связи обязаны осуществлять сбор и хранение служебной информации в порядке, определяемом Правительством Республики Казахстан. Однако закон не предписывает осуществлять сбор и хранение данных пользователей (переписка, звонки и т. д.)[12].

Среди основных задач по повышению уровня кибербезопасности М.Турин, эксперт по кибербезопасности Центра анализа и расследования кибератак (ЦАРКА), отмечает необходимость делать упор на образование. Также основной задачей в ближайшие несколько лет для Казахстана, по его оценке, является запуск 5 SOC и покрытие мониторингом всех критически важных объектов информационно-коммуникационной инфраструктуры. Кроме того, эксперт отмечает необходимость реформирования нормативной базы обеспечения кибербезопасности.

Республика Таджикистан

В Республике Таджикистан государственная политика в сфере информационной безопасности и кибербезопасности регулируется следующими актами:

- Концепция информационной безопасности Республики Таджикистан;
- Единая Концепция Республики Таджикистан по борьбе с терроризмом и экстремизмом;
- Закон Республики Таджикистан «Об информации»;
- Закон Республики Таджикистан «О защите информации»;
- Закон Республики Таджикистан «О борьбе с терроризмом»;

[12] Сабиров К.К., Ахмеджанов Ф.Р. Некоторые вопросы законодательного укрепления кибербезопасности в Республике Казахстан // Вопросы кибербезопасности. 2017. № 3 (21). С. 55–61.

- Закон Республики Таджикистан «О свободе совести и религиозных объединениях»;
- Закон Республики Таджикистан «О безопасности»;
- Государственная стратегия «Информационно-коммуникационные технологии для развития Республики Таджикистан»;
- Указ Президента Республики Таджикистан «О Национальной стратегии Республики Таджикистан по противодействию экстремизму и терроризму на 2016–2020 годы» и другие нормативные правовые акты.

Республика Таджикистан занимает седьмое место по уровню кибербезопасности в регионе СНГ согласно Глобальному индексу кибербезопасности (Global Cyber Security Index) на 2018 год и 107-е в глобальном рейтинге[13].

Базовым документом по информационной безопасности в Таджикистане является Концепция информационной безопасности Республики Таджикистан, утвержденная 7 ноября 2003 года.

Под информационной безопасностью Республики Таджикистан понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Выделяются четыре основные составляющие национальных интересов Республики Таджикистан в информационной сфере.

Первая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления республики, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя информационное обеспечение государственной политики, связанное с доведением до народа Таджикистана и

---

[13] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

международной общественности достоверной информации о государственной политике Республики Таджикистан, ее официальной позиции по социально значимым событиям республики и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя применение современных информационных технологий, создание отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Четвертая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории Республики Таджикистан.

Угрозы информационной безопасности Республики Таджикистан объединены в несколько групп:

– угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению Республики Таджикистан;

– угрозы созданию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории республики.

Законодательство Республики Таджикистан в сфере информационной безопасности развивается по следующим направлениям:

1) Закрепление общих положений о доступе к информации, о конфиденциальности и защите информации. Базовыми актами здесь

являются законы Республики Таджикистан «Об информации» и «О защите информации».

2) Определение правового режима отдельных видов информации:
   - семейной тайны и тайны личной жизни – Гражданский и Семейный кодексы Республики Таджикистан;
   - государственной тайны – Закон Республики Таджикистан «О государственных секретах»;
   - коммерческой тайны – Гражданский кодекс Республики Таджикистан и закон Республики Таджикистан «О коммерческой тайне»;
   - профессиональных, процессуальных тайн – процессуальные кодексы и законы о соответствующих видах деятельности (об адвокатуре, нотариате, охране здоровья граждан и т. п.).
3) Административное регулирование деятельности по защите информации, в том числе связанной с оборотом криптографических средств.
4) Определение порядка осуществления оперативно-разыскных мероприятий в информационной сфере.
5) Борьба с преступлениями в сфере информационной безопасности путем закрепления соответствующих составов преступлений в Уголовном кодексе Республики Таджикистан .

В Уголовном кодексе Республики Таджикистан содержатся следующие составы преступлений, которые можно отнести к киберпреступности:

▪ Неправомерный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, те же деяния, повлекшие по неосторожности изменение, уничтожение либо блокирование информации, а равно вывод из строя компьютерного оборудования, либо значительный ущерб.

▪ Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации, причинившее значительный ущерб или создавшее угрозу его причинения, то же деяние, сопряженное с неправомерным доступом к компьютерной системе или сети.

▪ Уничтожение, блокирование либо приведение в непригодное состояние компьютерной информации или программы, вывод из строя компьютерного оборудования, а равно разрушение компьютерной системы, сети или машинного носителя.

▪ Незаконное копирование или иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, а равно перехват информации, передаваемой с использованием компьютерной связи.

▪ Принуждение к передаче информации, хранящейся в компьютерной системе, сети или на машинных носителях, под угрозой оглашения позорящих сведений о лице или его близких, предания гласности сведений о таких обстоятельствах, которые потерпевший желает сохранить в тайне, а равно под угрозой применения насилия над лицом или его близкими либо под угрозой уничтожения или повреждения имущества лица, его близких и других лиц, в ведении или под охраной которых находится эта информация.

▪ Изготовление с целью сбыта, а равно сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети.

▪ Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, а также разработка специальных вирусных программ, заведомое их использование или распространение носителей с такими программами.

▪ Нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, если это повлекло по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования или причинение иного значительного ущерба.

Согласно Закону «О безопасности», принятому в 2014 году:

1. В Республике Таджикистан создается и укрепляется национальная система защиты информации, в том числе государственных информационных ресурсов.

2. Принятие решений органами и должностными лицами Республики Таджикистан по внешнеполитическим и внешнеэкономическим вопросам должно основываться на объективной и упреждающей информации о тенденциях мирового политического и экономического развития, ситуации в политике и экономике других государств, особенно сопредельных.

3. Обязанностью государственных органов, органов самоуправления поселков и сел, организаций, независимо от их организационно-правовой формы, должностных лиц и граждан является принятие всех необходимых мер по недопущению (Закон Республики Таджикистан от 15 марта 2016 года № 1283):

– информационной зависимости Таджикистана;

– информационной экспансии и блокады со стороны других государств;

– информационной изоляции органов государственной власти и сил обеспечения безопасности Республики Таджикистан.

4. Не допускается принятие решений и совершение действий, противоречащих национальным интересам формирования и бесперебойного функционирования информационного пространства Республики Таджикистан или вхождения Таджикистана в мировую систему связи и информатики.

5. Запрещается совершение нижеследующих действий:

– распространение на территории Республики Таджикистан печатной продукции, телевизионных программ и радиопередач зарубежных средств массовой информации, содержание которых подрывает национальную безопасность;

– разглашение служебной и иной информации, связанной с интересами государства.

В Национальной стратегии Республики Таджикистан по противодействию экстремизму и терроризму на 2016–2020 годы, принятой Указом Президента Республики Таджикистан от 12 ноября 2016 года, отмечается, что уровень информационно-просветительской, образовательной и идеологической работы по противодействию радикальной идеологии и экстремизму в стране требует усиления. В частности:

– не хватает специалистов в области информационного противодействия экстремизму и терроризму;

– существует дефицит информационной и справочной литературы по экстремистским и террористическим организациям, а также наглядной агитации и пропаганды;

– слаба роль средств массовой информации в предупреждении и профилактике экстремизма, а также в освещении антиэкстремистской и антитеррористической деятельности государственных органов.

В связи с этим отмечается необходимость принятия действенных мер по формированию мощного идеологического корпуса, укреплению его потенциала в предупреждении экстремизма и радикализации, подготовке специалистов в области информационного противодействия экстремизму и терроризму.

К наиболее значимым внешним источникам угроз, согласно оценкам экспертов, относятся:

– недружественная политика иностранных государств в области глобального распространения информации и новых информационных технологий;

– деятельность иностранных разведывательных и специальных служб;

– деятельность иностранных политических структур, направленная против интересов центральноазиатских государств;

– преступные действия международных групп, формирований и отдельных лиц, стремление ряда стран к доминированию и ущемлению интересов республик Центральной Азии в мировом информационном пространстве, вытеснению их с внешнего и внутреннего информационных рынков;

– деятельность международных террористических организаций;

– разработка рядом государств стратегий ведения информационных войн и создание технических средств и способов негативного воздействия на институты и структуры публичной власти страны[14].

К важнейшим внутренним источникам угроз относятся:

---

[14] Махмадов П.А. Информационная безопасность в системе политической коммуникации: состояние и приоритеты обеспечения (на материалах государств Центральной Азии) : дис. ... д-ра полит. наук : 23.00.04. Душанбе, 2018.

– критическое состояние отраслей промышленности;

– неблагоприятная криминогенная обстановка, сопровождающаяся усилением влияния организованной преступности на жизнь общества, снижением степени защищенности законных интересов граждан, общества и государства в информационной сфере;

– недостаточная координация деятельности органов государственной власти на местах по формированию и реализации единой государственной политики в области обеспечения информационной безопасности центральноазиатских республик.

Отмечается также, что отдельные недочеты наблюдаются при реализации Концепции информационной безопасности Республики Таджикистан. Основными из них являются следующие.

Во-первых, до сих пор на территории республики не налажено производство современных информационно-коммуникационных средств.

Во-вторых, мероприятия, направленные на обеспечение информационной безопасности Республики Таджикистан, финансируются недостаточно. Поэтому у министерств и ведомств республики нет финансовой возможности для проведения аттестации средств обработки имеющейся информации и их сертификации. Такое положение может отрицательно повлиять на эффективность обеспечения информационной безопасности.

Для улучшения процесса обеспечения информационной безопасности в качестве необходимых выделяются следующие шаги:

а) Министерству образования и науки Республики Таджикистан принять необходимые дополнительные меры для повышения уровня компьютерного образования, разработки и внедрения образовательных стандартов обучения информатике в учебных заведениях на всех уровнях и улучшения уровня подготовки специалистов и учителей по информационно-коммуникационным технологиям, как можно скорее решить вопрос обеспечения высококвалифицированными кадрами;

б) принять меры по формированию и реализации электронного Правительства, развитию механизмов внедрения электронной цифровой подписи в отраслях,

организовать республиканский Центр по идентификации электронной цифровой подписи и принять другие меры, направленные на развитие информационно-коммуникационных технологий.

Кыргызская Республика

Политика в сфере информационной безопасности формируется на основе следующих документов:

– Концепция цифровой трансформации «Цифровой Кыргызстан 2019–2023»;

– Стратегия кибербезопасности Кыргызской Республики на 2019–2023 годы;

– Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы;

– Концепция национальной безопасности Кыргызской Республики;

– Требования к защите информации, содержащейся в базах данных государственных информационных систем.

Нормативно-правовую базу обеспечения информационной безопасности формируют:

– Закон Кыргызской Республики «О защите государственных секретов Кыргызской Республики»;

– Закон Кыргызской Республики «Об электронном управлении»;

– Закон Кыргызской Республики «О гарантиях и свободе доступа к информации»;

– Закон Кыргызской Республики «О Национальном архивном фонде Кыргызской Республики»;

– Закон Кыргызской Республики «Об электрической и почтовой связи»;

– Закон Кыргызской Республики «Об электронной подписи»;

– Закон Кыргызской Республики «О средствах массовой информации»;

– Закон Кыргызской Республики «О правовой охране программ для ЭВМ и баз данных»;

– Закон Кыргызской Республики «Об основах технического регулирования в Кыргызской Республике»;

– Закон Кыргызской Республики «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики» и другие;

– Гражданский, Семейный, Уголовный и другие кодексы Кыргызской Республики;

– другие подзаконные акты, регламентирующие общественные отношения в информационной сфере.

Кыргызская Республика занимает восьмое место по уровню кибербезопасности в регионе СНГ согласно Глобальному индексу кибербезопасности (Global Cyber Security Index) на 2018 год и 111-е в глобальном рейтинге[15].

Кибербезопасность определяется как сохранение свойств целостности (которая может включать аутентичность и отказоустойчивость), доступности и конфиденциальности информации в объектах информационной инфраструктуры, обеспечиваемое за счет использования совокупности средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками и страхования, профессиональной подготовки, практического опыта и технологий.

В действующей Концепции национальной безопасности Кыргызской Республики, которая была утверждена Указом Президента Кыргызской Республики от 12 июня 2012 года, заложены и вопросы обеспечения информационной безопасности.

В частности, в отдельном параграфе Концепции «Недостаточная развитость информационно-коммуникационных технологий и слабая защита информационного пространства страны» отмечается, что «недостаточное внимание уделяется вопросам формирования и реализации единой государственной политики по обеспечению информационной безопасности, координации деятельности органов власти и управления Кыргызской Республики по укреплению информационной безопасности. Мероприятия, нацеленные на защиту информационной сферы, недостаточно обеспечены финансовыми ресурсами.

---

[15] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Вследствие вышеназванных причин в Кыргызской Республике наблюдается усиление угроз национальной безопасности Кыргызской Республики в информационном пространстве страны по следующим направлениям:

– стремление сопредельных государств к доминированию в информационном пространстве Кыргызской Республики (включая получение доступа к информации с ограниченным доступом) и как следствие вытеснение его из внутреннего рынка;

– увеличение технологического отрыва от ведущих мировых держав, усиливающее зависимость Кыргызской Республики от закупок зарубежной техники для обеспечения важных национальных информационных инфраструктур;

– деятельность международных экстремистских, террористических и других преступных сообществ, антиобщественных организаций и групп в информационной сфере Кыргызской Республики, их интерес к обладанию информационным оружием и его применению».

Сфера обеспечения информационной безопасности отмечается также в списке перспективных направлений развития законодательства. Такое развитие предполагает создание эффективных государственных механизмов по обеспечению информационной безопасности, а также участие в этой деятельности гражданского общества.

Среди необходимых мер предупреждения и нейтрализации внешних и внутренних угроз отмечается:

– расширение спектра информационных услуг, оказываемых библиотеками с широким применением новых информационных технологий;

– формирование национальной информационной политики и разработка национальной стратегии по информационным технологиям, совершенствование системы информационного обеспечения во всех сферах жизнедеятельности и регионах страны;

– усиление координации деятельности органов власти и управления Кыргызской Республики по укреплению информационной безопасности;

– развитие государственной сети радиомониторинга.

Выделяются следующие виды угроз в информационной сфере:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению Кыргызской Республики;
- угрозы информационному обеспечению государственной политики Кыргызской Республики;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории Кыргызской Республики.

Основными направлениями обеспечения информационной безопасности выступают:

1) правовое обеспечение (применение правовых норм обеспечения безопасности);
2) организационное обеспечение (регламентация деятельности, исключающая нанесение ущерба; наличие соответствующих служб);
3) инженерно-техническое обеспечение (использование технических средств, препятствующих нанесению ущерба, физические, аппаратные, программные и криптографические средства защиты).

В Концепции национальной безопасности Кыргызской Республики определяются следующие национальные интересы Кыргызстана в информационной сфере:

– защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории Кыргызской Республики;

– развитие современных информационных технологий, отечественной ИКТ-индустрии, обеспечение потребностей внутреннего рынка ее продукцией и выход этой

продукции на мировой рынок, а также обеспечение накопления, сохранения и эффективного использования отечественных информационных ресурсов;

– информационное обеспечение государственной политики Кыргызской Республики по доведению до национальной и международной общественности достоверной информации о государственной политике Кыргызской Республики с обеспечением доступа к открытым государственным информационным ресурсам;

– соблюдение прав и свобод человека в информационной сфере, обеспечение духовного обновления в Кыргызской Республике, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

К основным внешним источникам угроз в информационной сфере относятся:

– деятельность иностранных политических, экономических, военных, разведывательных и информационных структур;

– стремление ряда стран к доминированию и ущемлению интересов Кыргызской Республики;

– обострение международной конкуренции за обладание информационными технологиями и информационными ресурсами;

– деятельность международных террористических организаций;

– увеличение технологического отрыва ведущих стран мира;

– разработка рядом государств концепций информационных войн.

Среди внутренних источников угроз в информационной сфере выделяются:

– недостаточная разработанность нормативно-правовой базы, недостаточная правоприменительная практика, неразвитость институтов гражданского общества;

– недостаточное бюджетное финансирование мероприятий по обеспечению информационной безопасности Кыргызской Республики;

– недостаточная экономическая мощь государства;

– дефицит квалифицированных кадров;

– отставание от других стран в области создания и внедрения ИКТ, развития индустрии информационных услуг и широкое использование зарубежных программно-аппаратных средств;

– стремление организованных деструктивных сил к получению доступа к информационным ресурсам.

Концепция цифровой трансформации «Цифровой Кыргызстан 2019–2023» была принята в 2018 году с целью консолидации усилий государства, гражданского общества и бизнеса по ускорению цифровой трансформации государства и создания достаточных институциональных и инфраструктурных условий для перехода к цифровой экономике.

В разделе 4.2.2 «Формирование и укрепление доверия и обеспечение безопасности при использовании технологий» отмечается необходимость применения стратегического подхода к кибербезопасности, при котором видение страны в отношении социально-экономического развития в полной мере соответствует ее повестке в области цифровой безопасности. Вопросы кибербезопасности следует решать, принимая во внимание глобальный, транснациональный характер киберугроз. Речь идет об утверждении национальной стратегии кибербезопасности вместе с планом действий по ее реализации в горизонте до 2023 года.

Целью Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы и Плана мероприятий по ее реализации является формирование отечественной системы и политики кибербезопасности для обеспечения соответствующего уровня безопасности граждан, бизнеса и государства, позволяющего защитить их жизненно важные интересы в киберпространстве и обеспечить устойчивое социально-экономическое развитие Кыргызской Республики, включая цифровую трансформацию экономики.

К задачам, указанным в Стратегии и Плане мероприятий, относятся:

1) формирование основы для единой системы и политики обеспечения кибербезопасности Кыргызской Республики;

2) формирование единого понятийного и методологического аппарата в области кибербезопасности;

3) сокращение количества и минимизация последствий компьютерных инцидентов на объектах информационной инфраструктуры Кыргызской Республики за

счет формирования и развития отечественной системы предупреждения, реагирования и управления компьютерными инцидентами;

4) формирование организационно-технической и нормативно-правовой основы системы тестирования и сертификации средств защиты информации, включая средства криптографической защиты информации;

5) модернизация системы национальных стандартов в области кибербезопасности и защиты информации;

6) повышение уровня кадрового потенциала для реализации государственной политики Кыргызской Республики в области обеспечения кибербезопасности.

Законом Кыргызской Республики от 24 января 2017 года № 10 были внесены изменения и дополнения в Уголовный кодекс Кыргызской Республики. В новой редакции Уголовного кодекса Кыргызской Республики, которая вступила в силу с 1 января 2019 года, глава, посвященная преступлениям в сфере информационной безопасности, дополнена такими видами преступлений, как неправомерный доступ к компьютерной информации и компьютерный саботаж.

Среди основных недостатков законодательства в сфере кибербезопасности отмечаются следующие[16]:

– в законодательстве Кыргызской Республики нет четкого определения таких терминов, как кибербезопасность, киберпространство, кибергигиена, критическая инфраструктура и т. д.;

– отсутствует уполномоченный государственный орган для обеспечения кибербезопасности в виде созданной и полноценно функционирующей структуры по реагированию на возникающие угрозы и киберинциденты (CERT); иерархия государственных структур, задействованных в данной сфере (Совет безопасности (обороны), Государственный комитет национальной безопасности, Министерство внутренних дел, Государственный комитет информационных технологий и связи), не выстроена четким образом, с точным и ясным распределением задач и функций в информационной сфере;

---

[16] Анализ действующего законодательства, регулирующего кибербезопасность, и выявление ключевых пробелов с рекомендациями, Общественный фонд «Гражданская инициатива интернет-политики».

– Кыргызская Республика довольно слабо представлена в международных договорах и соглашениях в сфере обеспечения информационной безопасности и кибербезопасности (за исключением Соглашения государств – членов Шанхайской организации сотрудничества; в рамках ОДКБ работа только начата);

– несмотря на то, что во многих учебных заведениях страны имеются программы обучения по вопросам информационной безопасности, подготовка отечественных специалистов в сфере обеспечения и регулирования кибербезопасности не осуществляется, а обучающие программы по информационной безопасности не отвечают требованиям сегодняшнего дня;

– отсутствуют возможности для защиты критической инфраструктуры, поскольку само понятие «критическая информационная инфраструктура» не содержится в действующем законодательстве (есть фрагментарно урегулированные вопросы, касающиеся стратегических объектов, в том числе телекоммуникационных);

– не разработана специализированная иерархия уровней кибербезопасности.

Согласно Закону Кыргызской Республики «О Совете обороны Кыргызской Республики» Совет обороны вырабатывает решения по подготовке к защите Кыргызской Республики от современных вызовов и угроз.

В целом, по оценке эксперта Общественного фонда «Гражданская инициатива интернет-политики» Т.Мамбеталиевой[17], анализ действующего законодательства в сфере информационной безопасности позволяет сделать выводы о том, что оно:

1) представляет собой устаревшую базу, не содержит терминов и определений информационной безопасности, кибербезопасности, киберпространства, кибергигиены, понятий критической инфраструктуры и т. п.;

2) в определенной степени остается противоречивым, отражая ведомственные интересы, и не подкреплено реальными ресурсами;

3) не обеспечивает эффективного контроля за соблюдением прав субъектов правовых отношений.

Кроме того, экспертами фонда отмечается необходимость создания Концепции (Стратегии) по кибербезопасности.

---

[17] Интервью проведено в рамках исследования.

Также отмечается, что на основе международной практики и опыта зарубежных стран необходимо дополнить уголовное законодательство нормами, устанавливающими ответственность за совершение преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем, деяний, связанных с подлогом компьютерных данных, и других противоправных действий, способных причинить тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом. К таким преступлениям можно отнести: незаконный доступ к компьютерной системе или к ее части; умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему; незаконное вмешательство в данные путем умышленного повреждения, стирания, порчи, изменения или подавления компьютерных данных; подлог компьютерных данных, компьютерное мошенничество и т. п[18].

Основные вызовы и существующие угрозы, общие подходы и приоритетные направления

Учитывая интенсивное развитие информационных технологий в мире, внедрение автоматизированных автономных систем управления в многочисленных отраслях, а также сферах стратегического значения, массовое распространение коммуникационных систем, увеличение объемов торговых, финансовых оборотов в электронном формате, всемирные тенденции накапливания и использования информации, в том числе и персональных данных, обозначим ряд важных вопросов, которые включены в данную концепцию.

1. Усовершенствование и гармонизация правового поля в сфере кибербезопасности в государствах – членах Организации Договора о коллективной безопасности.

2. Сотрудничество по обеспечению и усовершенствованию правовых норм («киберзаконов») в сферах управления производственными механизмами,

[18] Анализ действующего законодательства, регулирующего кибербезопасность, и выявление ключевых пробелов с рекомендациями, Общественный фонд «Гражданская инициатива интернет-политики».

обслуживающими и бытовыми электронными приборами и роботами, транспортными, в том числе судоходными и авиационными, средствами.

3. Разработка общей законодательной базы по безопасности в киберпространстве, обеспечивающей защиту от ряда рисков при использовании данных, предоставляемых космическими спутниками, при пользовании социальными сетями, электронной почтой, в том числе государственной и дипломатической перепиской, и отдельными коммуникационными порталами и чатами.

4. Необходимость принятия мер по обеспечению защитных «киберзаконов», относящихся к сфере здравоохранения, к области управления оборонными системами, а также касающихся автоматизированных и программируемых избирательных процессов.

5. Безотлагательное обеспечение взаимодействия стран ОДКБ и международных структур с целью усиления правового контроля за электронными финансовыми операциями, оборотами электронной торговли, интернет-зонами азартных игр.

Признавая тенденцию увеличения масштабов нарушений и преступлений в киберпространстве, считаем необходимым отметить следующие существующие риски:

1) вымогательство путем использования незаконного доступа к компьютерам, мобильным устройствам, аккаунтам в социальных сетях и кабинетам на общедоступных сайтах и т. д.;

2) хулиганство, распространение материалов незаконного характера, подстрекательство, пропаганда насилия, терроризма и призывы к насильственным действиям;

3) распространение наркотических средств, формул синтетических наркотиков (спайсов) и другой информации по изготовлению различных наркотиков;

4) мошенничество, обманные операции с движимым и недвижимым имуществом, драгоценными металлами и камнями, антиквариатом и т. д.;

5) финансовые пирамиды, отмывание денежных средств, незаконные азартные игры, ложные лотереи, подставные или нереальные брокерские махинации, продажа несуществующих на реальном рынке ценных бумаг и т. д.;

6) фальшивые аукционы, не существующие в реальной жизни интернет-магазины, ложные благотворительные акции;

7) преследование, незаконный сбор персональных данных и их использование, идентификация лиц;

8) незаконное прослушивание голосовых переговоров или отслеживание и просмотр переписок, а также фото- и видеоматериалов;

9) предложение незаконных или нереальных услуг мошеннического характера;

10) международная, военная, промышленная, деловая, политическая шпионская деятельность;

11) распространение вирусов (вредоносных программ) с целью вредительства либо в рамках одного или нескольких вышеперечисленных пунктов.

Поскольку при реализации почти всех перечисленных преступлений или незаконных действий злоумышленники в общей цепи событий частично или полностью действуют в интернет-пространстве, то нередко их действия выпадают за рамки уголовного права, регулирующего ответственность за преступления в реальной жизни по причине отсутствия законов, относящихся к конкретным действиям в Интернете или с использованием Интернета. С учетом существования отдельных законов, относящихся к противодействию преступлениям в киберпространстве в ряде стран ОДКБ, а также соответствующей конвенции Совета Европы, соглашения Организации Объединенных Наций, договора стран НАТО и поправок к указанным документам, очевидна необходимость определенной детализации «киберзаконов» относительно существующих рисков и имеющих место преступлений. Необходимо своевременно разработать и принять такие законодательные акты, которые регулировали бы преступления, совершаемые посредством Интернета или при частичном использовании глобальной сети. Подчеркивая важность своевременного принятия законодательства в странах ОДКБ в соответствии с требованиями современного демократического общества и правового общественного сознания мирового сообщества, настоятельно рекомендуем парламентам государств – членов ОДКБ разработать «киберкодекс» (подробное законодательство по кибернетической безопасности), а с целью регулирования и совершенствования международного

законодательства в сфере безопасности в киберпространстве Парламентской Ассамблее ОДКБ приступить к разработке проекта Конвенции по кибербезопасности.

Нормативно-правовое регулирование вопросов кибербезопасности в Евросоюзе

Европейская стратегия безопасности была принята в декабре 2003 года. Уже в 2013 году киберугрозы и необходимость их предотвращения были названы важнейшими в ряду других проблем безопасности ЕС. Именно с этого времени Евросоюз пытался разработать соответствующую программу цифровой и информационной безопасности.

Первая Стратегия ЕС в области кибербезопасности (2013 года) решала две задачи – профилактика киберпреступлений и реагирование на атаки в телекоммуникационных системах Европы. Она была подготовлена совместно Генеральным директоратом Европейской комиссии по коммуникационным сетям, контенту и технологиям (DG Connect), Генеральным директоратом по миграции и внутренним делам (DG HOUM)и Европейской службой внешних связей. Стратегия выделяет пять векторов развития сферы:

1) достижение киберстрессоустойчивости;
2) снижение уровня киберпреступности;
3) развитие кибersоставляющей политики безопасности и обороны;
4) обеспечение промышленными и технологическими ресурсами;
5) развитие последовательной международной политики ЕС в области кибербезопасности с продвижением европейских ценностей.

Стратегия вводила минимальные стандарты безопасности для всех цифровых и информационных систем.

Стоит также отметить, что в борьбе с киберпреступностью важнейшую роль играет Европейская комиссия. Она, в дополнение Стратегии ЕС, еще в 2013 году разработала Директиву о кибербезопасности (директива ЕС, в отличие от регламента, требует трансформации во внутреннее право, то есть не действует напрямую), которая предполагала объединение усилий частного сектора и национальных правительств в

сотрудничестве с соответствующими структурами Европейского союза для обеспечения кибербезопасности. Директива указала на необходимость минимальной гармонизации правовой базы государств – членов ЕС в данной сфере. Однако основная ответственность осталась на национальных правительствах.

Свое слово в борьбе с киберугрозами сказал и Европарламент, одобрив в марте 2014 года предлагаемую Еврокомиссией повестку кибербезопасности.

В 2014–2015 годах к данному процессу присоединился и Совет ЕС. К маю 2016 года он разработал Правила кибербезопасности для ЕС – «Директиву о сетевой и информационной безопасности» (NIS). Согласно документу обеспечение безопасности возлагается на конкретных операторов, прежде всего в критически значимых секторах (финансы, транспорт, энергетика, здравоохранение). Каждая страна обязана обеспечивать собственную безопасность и, таким образом, безопасность своих партнеров.

В соответствии с Директивой NIS также создается Стратегическая группа сотрудничества, а на национальном уровне утверждаются свои группы реагирования и агентства кибербезопасности, которые обязаны сотрудничать с аналогичными структурами в других государствах ЕС.

Важнейшим координирующим положением Директивы можно считать создание сети групп реагирования на инциденты компьютерной безопасности (CSIRTs). В сеть должны входить соответствующие подразделения каждого из государств – членов ЕС. Европейское агентство по сетевой и информационной безопасности намерено активно поддерживать сотрудничество между этими группами.

Согласно статье 25 Директивы NIS государства – члены ЕС должны принять соответствующие законодательные положения для выполнения требований Директивы. В силу положений пункта 2 статьи 1, статьи 7 Директивы NIS государства-члены должны принять национальные стратегии по обеспечению безопасности сетевых и информационных систем, а также установить требования к соответствующим субъектам, в частности определить критерии оценки возможного негативного воздействия и установить параметры группирования таких субъектов в зависимости от этих критериев.

Европейский союз активно развивал и продолжает развивать нормативную базу кибербезопасности. При этом приверженность ЕС принципам прав и свобод человека проходит красной нитью через все документы о кибербезопасности.

Другим известным нормативным актом, инициированным Генеральным директоратом по правосудию и защите потребителей, стал Регламент по защите персональных данных, вступивший в силу в 2018 году. Этим документом был утвержден принцип свободной передачи информации между государствами – членами ЕС. Кроме того, инновацией стало обязательство операторов персональных данных предусматривать необходимые меры по их защите, а также информировать органы власти о нарушениях конфиденциальности.

В марте 2019 года Европейский парламент одобрил Акт по кибербезопасности (Cybersecurity Act) – пакет документов, направленных на законодательное усиление системы кибербезопасности ЕС. Акт внедряет стандарты кибербезопасности в правила функционирования единого рынка, а также усиливает роль Европейского агентства по сетевой и информационной безопасности, гарантируя ему постоянный мандат.

Наряду с Европейским агентством по сетевой и информационной безопасности (включая создаваемые команды по координации и сотрудничеству) вопросами кибербезопасности занимаются такие институты Евросоюза, как ЕВРОПОЛ, Европейский центр по борьбе с киберпреступностью (главный инструмент по борьбе с кибератаками в ЕС) (в рамках ЕВРОПОЛа), Команда срочного компьютерного реагирования для институтов ЕС (the Computer Emergency Response Team for the EU institutions). Ключевыми в этой сфере также являются Генеральный директорат помиграции и внутренним делам и Генеральный директорат по правосудию и защите потребителей.

С 2004 года Европейское агентство по сетевой и информационной безопасности – центральный институт в области кибербезопасности. Агентство в основном осуществляет анализ ситуации и разрабатывает рекомендации.

Для поддержки кибербезопасности ЕС взаимодействует с такими структурами, как Организация экономического сотрудничества и развития, Генеральная Ассамблея

ООН, Международный союз электросвязи, ОБСЕ, Саммит информационного общества, Форум управления в Интернете. Центральным остается сотрудничество ЕС с НАТО.

Нормативное регулирование кибербезопасности в некоторых странах ЕС

Эстонская Республика

Опыт Эстонской Республики в реализации политики кибербезопасности является одним из передовых. В государстве разрабатываются и принимаются стратегические документы в этой сфере, созданы соответствующие институциональные структуры.

В 2008 году Эстония одна из первых в мире приняла Национальную стратегию кибербезопасности, вписанную в рамки международного права. Стратегия кибербезопасности на 2014–2017 годы – это основной документ для планирования кибербезопасности Эстонии и часть общей стратегии безопасности Эстонской Республики. Стратегия освещает важные достижения, оценивает угрозы кибербезопасности и содержит перечень мероприятий для борьбы с этими угрозами.

Федеративная Республика Германия

В 2011 году правительство опубликовало первую версию документа «Кибербезопасность для Германии» (Cyber Security Strategy for Germany). В этом документе признается зависимость между информационно-коммуникационными технологиями (ИКТ) и экономическим и социальным ростом в стране и указывается, что Интернет, а также ИКТ являются критической инфраструктурой для германского общества.

Национальная стратегия кибербезопасности выделяет несколько стратегических областей и целей для более успешной борьбы с киберугрозами: защита критических элементов инфраструктуры и ИТ-систем; защита ИТ-систем общественного управления посредством создания единой федеральной сети; создание Национального центра киберреагирования (National Cyber Response Center) для реагирования на инциденты и защиты данных и систем; создание Совета национальной кибербезопасности (National

Cyber Security Council) для активизации сотрудничества между организациями государственного и частного секторов; развитие активного международного сотрудничества для координации деятельности по обеспечению кибербезопасности; разработка и создание надежных ИТ-продуктов с использованием инноваций; подготовка и тренинг персонала федеральных органов власти; эффективное использование инструментария государственных органов – таких как законодательство – для борьбы с киберпреступностью.

Кроме того, документ определил Федеральное управление по информационной безопасности Министерства внутренних дел (Bundesamt für Sicherheit in der Informationstechnik, BSI) органом, ответственным за кибербезопасность страны и за реализацию указанной стратегии. Управление было создано в 1991 году для предоставления услуг в области ИТ-безопасности федеральному правительству, ИКТ-компаниям, частным и коммерческим пользователям, а также интернет-провайдерам Германии. Как требовала Национальная стратегия, BSI создало Национальный центр киберреагирования (Nationales Cyber-Abwehrzentrum, NCAZ), ответственный за определение, анализ и разработку мер, необходимых для нивелирования и устранения потенциальных угроз.

Цифровая повестка Германии от 2014 года (Digital Agenda 2014–2017) повторяет основные элементы Национальной стратегии кибербезопасности, также признавая важность ИКТ для экономического роста и одновременно подчеркивая необходимость повышения уровня безопасности в киберпространстве. Так, в настоящее время BSI работает над реализацией Акта об ИТ-безопасности от 2015 года (IT Security Act) – ключевого элемента национальной стратегии ИТ-развития и ее положений по защите критической инфраструктуры национального значения. Эта деятельность предполагает постоянное сотрудничество с операторами критически важных элементов инфраструктуры с целью определения минимальных стандартов безопасности для таких компаний и секторов экономики в целом, а также с целью повышения доступности, адекватности, конфиденциальности и целостности системы ИТ-безопасности по всей стране.

И стратегия кибербезопасности, и «цифровая повестка» представляют собой попытки создания всеобъемлющего и многостороннего подхода в деле повышения безопасности онлайн-услуг и критически важных элементов инфраструктуры. Вместе с тем правительству Германии еще предстоит многое сделать для повышения уровня координации и взаимодействия между ведущими государственными и частными организациями, а также национальными ИТ-системами, чтобы быть более подготовленными к новым рискам, связанным со все растущей компьютеризацией критически важных услуг в национальной экономике.

Французская Республика

Кибербезопасность во Французской Республике регламентируется Национальной стратегией цифровой безопасности Франции, Белой книгой и рядом законов, таких как Закон о военном программировании.

Национальная стратегия цифровой безопасности Франции

Национальная стратегия цифровой безопасности Франции, представленная в 2015 году премьер-министром М.Вальсом и предназначенная для поддержки цифрового перехода французского общества, делает республику лидером в продвижении европейской цифровой стратегической автономии.

Эта стратегия является результатом скоординированных межведомственных усилий по реагированию на возникающие проблемы цифрового перехода, который способствует инновациям и росту, но в то же время несет риски для государства и граждан. Киберпреступность, шпионаж, пропаганда, саботаж и чрезмерная эксплуатация личных данных угрожают цифровому доверию и безопасности, что требует коллективного и скоординированного реагирования.

Белая книга 2008 года по обороне и национальной безопасности

В связи с постоянным ростом зависимости от ИТ-процессов, обусловленной развитием информационного общества и все более широким использованием

информационных технологий в важнейших процессах жизни государства и общества, в 2008 году Президент Франции Н.Саркози принял решение о создании Белой книги по обороне и национальной безопасности. В ней должны были быть изложены угрозы, с которыми сталкивается нация, и определен потенциал, необходимый для противодействия этим угрозам.

Белая книга 2008 года, подчеркивая потенциально огромное влияние кибератак на жизнь нации, одним из главных приоритетов государства в обеспечении национальной безопасности назвала развитие потенциала для предотвращения кибератак и реагирования на них. В частности, в области киберзащиты отмечена необходимость раннего обнаружения кибератак и организации противодействия таким атакам.

В соответствии с предложениями Белой книги было создано Национальное агентство безопасности информационных систем (ANSSI), по решению которого был образован комитет по кибербезопасности для разработки национальной стратегии в этой области.

Наряду с созданием ANSSI, соответственно положениям Белой книги, для каждой сферы обороны и безопасности на национальной территории была создана зональная обсерватория кибербезопасности (OzSSI). Целью таких обсерваторий стало общенациональное внедрение мер, принятых для повышения кибербезопасности.

Белая книга 2013 года по обороне и национальной безопасности
и закон о военном программировании

В 2013 году была опубликована новая Белая книга, которая характеризуется усилением мер по обеспечению кибербезопасности, прежде всего в отношении сетей операторов и информационных систем, имеющих жизненно важное значение. В связи с этим Белой книгой предписано, в частности:

– соблюдать стандарты безопасности, определенные ANSSI при взаимодействии с операторами;

– иметь надежные механизмы обнаружения, управляемые ANSSI, или покупать услуги у надежных поставщиков;

– сообщать о серьезных инцидентах в ANSSI.

Закон о военном программировании, принятый в декабре 2013 года, соответствовал руководящим принципам, установленным в Белой книге 2013 года по обороне и национальной безопасности. Этот законодательный механизм предоставил национальным операторам государственного и частного секторов, имеющим жизненно важное значение, возможности для лучшей защиты себя, а ANSSI – для более эффективной поддержки других государственных органов в случае кибератак. Статья 22 Закона предусматривает принятие мер по усилению безопасности операторов, имеющих жизненно важное значение, и наделяет премьер-министра новыми полномочиями.

Республика Польша

В Доктрине кибербезопасности Республики Польша, принятой в январе 2015 года, определены стратегические направления действий для обеспечения безопасности республики в киберпространстве. В то же время доктрину следует рассматривать как единую концептуальную базу, которая обеспечивает системный и комплексный подход к проблеме киберзащиты и кибероборонь, – как общий знаменатель для действий, осуществляемых субъектами государственной администрации, службами безопасности и общественного порядка, вооруженными силами, частным сектором и гражданами. Благодаря этому Доктрина кибербезопасности может стать отправной точкой для дальнейшей работы по укреплению безопасности Польши.

1. Общие положения

В современном мире, характеризующемся проникновением информационных технологий практически во все сферы жизнедеятельности человека и государства, кибербезопасность стала неотъемлемой частью обеспечения национальной безопасности. Разработка и периодическое редактирование нормативно-правовой базы и инструментария, способного реагировать на интенсивно прогрессирующие вызовы и

угрозы в киберпространстве, является важнейшей государственной задачей для каждого из государств – членов Организации Договора о коллективной безопасности.

Вызовы и угрозы в сфере кибербезопасности касаются весьма широкого спектра вопросов – от незаконного доступа к личным данным и нарушения прав и свобод личности до проникновения в механизмы регулирования инфраструктуры государства и нанесения колоссального вреда, в том числе создания угроз жизни и физической безопасности.

Каждое из государств – членов ОДКБ на протяжении ряда лет формировало и модифицировало свои инструменты реагирования на вызовы в этой сфере. Однако, с учетом трансграничности многих вызовов и глобальности угроз, с которыми сталкиваются все члены Организации и другие страны мира, очевидна необходимость координации действий и оказания поддержки друг другу как в виде обмена информацией, так и путем совмещения наиболее успешного опыта и продуктивных мер.

Концепция плана действий и инструментария в вопросах противодействия кибервызовам и угрозам представляет собой систему взглядов на возможные согласованные действия и инструменты, которые будут применяться одновременно во всех государствах – членах Организации Договора о коллективной безопасности и помогут совместить усилия по борьбе с киберпреступностью и повысить уровень кибербезопасности на всем пространстве ОДКБ.

Основу настоящей Концепции составляют конституции государств – членов ОДКБ, общепризнанные принципы и нормы международного права, национальные законодательные и иные нормативные правовые акты государств – членов ОДКБ, а также международные договоры в области кибербезопасности.

Целью Концепции является формирование условий для координации действий в процессе противодействия кибервызовым и угрозам, создание упорядоченной и унифицированной правовой базы для внедрения единого инструментария и повышения эффективности сотрудничества в сфере обеспечения кибербезопасности.

В Концепции не приводится глоссарий основных понятий и терминов, так как изучение национальных законодательных баз и стратегических документов,

регулирующих сферу информационной безопасности, показало отсутствие единых подходов к основополагающим вопросам, в том числе и понятиям. Разработка единого категориального аппарата должна стать одним из первых шагов к формированию единых подходов и инструментария.

Концепция является основой для разработки и реализации специальных планов и программ в области повышения эффективности сотрудничества в сфере кибербезопасности, обоснования распределения необходимых кадровых, материальных и иных ресурсов.

Подготовка Концепции основывалась на изучении и анализе нормативных актов, основополагающих документов стратегического планирования государств – членов ОДКБ в сферах обеспечения национальной безопасности, информационной безопасности, защиты государственных секретов, развития информационного общества, противодействия преступлениям в информационной сфере, развития информационной инфраструктуры, деятельности средств массовой информации и др. Содержание настоящей Концепции согласовано с положениями модельных законодательных актов и рекомендаций, принятых Межпарламентской Ассамблеей государств – участников Содружества Независимых Государств, и основополагающих международных правовых документов в данной области.

2. Цели и принципы плана действий и инструментария в вопросах противодействия кибервызовам и угрозам в государствах – членах ОДКБ

Совместная деятельность государств – членов ОДКБ в сфере обеспечения информационной безопасности имеет своей целью более эффективную защиту их законных интересов в информационной сфере. Такая деятельность направлена прежде всего на создание правовых условий для системной реализации и обеспечения защиты сбалансированных интересов личности, общества и государства в рамках государственной политики обеспечения кибербезопасности.

Целями плана действий и инструментария в вопросах противодействия кибервызовам и угрозам являются:

1) выработка наиболее эффективных правовых механизмов комплексного противодействия кибервызовам и угрозам, укрепления законности и правопорядка;

2) сочетание международных и государственных мер противодействия кибервызовам и угрозам;

3) совершенствование взаимодействия государств – членов ОДКБ по обеспечению кибербезопасности, оперативного реагирования на возникновение новых угроз и повышения эффективности применяемых механизмов;

4) создание условий для равноправного участия государств – членов ОДКБ в мировых информационных отношениях.

В свете решения указанных задач исключительно важным является вопрос проработки и однозначного толкования правовых понятий для сферы информационной безопасности, разработки единого категориального аппарата.

Общими принципами противодействия кибервызовам и угрозам являются:

– учет и обеспечение интересов государств – членов ОДКБ в информационной сфере, совместимость с задачами поддержания международной безопасности и стабильности;

– направленность правового регулирования отношений по обеспечению информационной безопасности на обеспечение социального и экономического развития государств;

– обеспечение незыблемости суверенитета и юрисдикции каждого государства – члена ОДКБ;

– паритетное участие государств – членов ОДКБ в отношениях по обеспечению кибербезопасности;

– развитие норм международного права в системе законодательства государств – членов ОДКБ;

– добровольное принятие и исполнение каждым государством – членом ОДКБ обязательств, касающихся совместного обеспечения кибербезопасности;

– взаимное неприменение мер информационной агрессии и информационной экспансии в межгосударственном сотрудничестве.

В основу разрабатываемого плана действий и инструментария должны быть заложены и следующие принципы:

– сбалансированность прав, свобод и обязанностей личности, общества и государства в сфере обеспечения кибербезопасности;

– свобода создания, сбора, хранения, использования и распространения информации любым законным способом;

– гармонизация и интеграция с международными системами кибербезопасности;

– открытость деятельности по обеспечению кибербезопасности, предусматривающая информирование общества об обеспечении информационной безопасности с учетом ограничений, установленных законодательством.

Специальным принципом является динамичное совершенствование правовых методов и механизмов реагирования на киберугрозы и вызовы.

3. Общие кибервызовы и угрозы для государств – членов ОДКБ

В целях разработки наиболее эффективного инструментария для противодействия кибервызовам и угрозам на пространстве ОДКБ необходимо выделить общие для государств – членов ОДКБ вызовы и угрозы, получившие свое отражение в законодательстве и стратегическом планировании стран, а также вызовы и угрозы, не получившие полноценного правового регулирования или практического решения в государствах – членах ОДКБ.

3.1. Общие для государств – членов ОДКБ вызовы и угрозы, отраженные в законодательстве:

– использование трансграничного оборота информации для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности;

– наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях, осуществление технической разведки в отношении государственных органов, научных организаций и предприятий оборонно-промышленного комплекса стран ОДКБ;

– использование средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в регионе;

– использование со стороны террористических и экстремистских организаций механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников;

– рост преступности с использованием информационно-коммуникационных технологий, прежде всего в кредитно-финансовой сфере, рост числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий;

– утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности;

– увеличение масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, безопасности государств – членов ОДКБ и представляющих угрозу всему миру, глобальной и региональной безопасности;

– нарастание информационного противоборства, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

– недостаточная эффективность информационного обеспечения государственной политики;

– нарушение функционирования критически важных информационных инфраструктур, деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов государств – членов ОДКБ путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру;

– снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента, высокий уровень зависимости промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития государств – членов ОДКБ от геополитических интересов зарубежных стран;

– недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

– низкий уровень кадрового обеспечения в области информационной безопасности;

– недостаточный уровень информационно-правовой культуры и образования в области информационной безопасности;

– низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности.

3.2. Вызовы и угрозы, не получившие полноценного правового регулирования или практического решения в государствах – членах ОДКБ:

– неэффективность методов и инструментария по раскрытию и расследованию преступлений с использованием информационно-телекоммуникационных технологий, вызванная их недостаточно оперативной модернизацией;

– затрудненный обмен информацией между разными странами при учете трансграничности киберпреступности, большие временные затраты на оформление и согласование документов при непродолжительности хранения следов преступной деятельности в инфраструктуре Интернета (источники информационных угроз могут находиться вне юрисдикции законодательства государств – членов ОДКБ);

– недостаточная правовая урегулированность деятельности государственных учреждений, проводящих компьютерно-технические и иные судебные экспертизы по делам о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий;

– несформированность предмета, методов, целей и задач цифровой криминалистики, отсутствие практических рекомендаций по работе с электронными, виртуальными, цифровыми следами, компьютерной техникой, интернет-сервисами, приложениями и программным обеспечением;

– отсутствие эффективного взаимодействия органов внутренних дел с государством, обществом и учреждениями, например отсутствие сформированной системы оперативного обмена информацией с банковскими организациями, финансово-кредитными учреждениями и даже с операторами сотовой связи, необходимой для раскрытия преступлений;

– недостатки правового регулирования постоянно развивающейся сферы киберпреступлений, отсутствие механизмов борьбы с преступлениями, совершаемыми с использованием анонимных и неконтролируемых сервисов, использованием приложений-мессенджеров в преступных целях, «серых» сим-карт;

– отсутствие стандартов обеспечения информационной безопасности государственных органов и частных компаний, использование несертифицированного оборудования и программного обеспечения (ПО), несоблюдение правовых, организационных и технических требований;

– бурное развитие телекоммуникационной сферы, ведущее к более глубокому проникновению в киберпространство инфраструктур страны, что в свою очередь создает множество новых уязвимых узлов;

– распространение высокоскоростных мобильных сетей 5-го поколения и связанная с этим возможность увеличения массовости кибератак;

– оснащение бытовых приборов различными технологиями для взаимодействия между собой или с внешней средой («интернет вещей»), что увеличивает возможности для использования всех этих устройств и образуемых ими сетей в качестве плацдарма для хакерских атак, незаконного доступа к конфиденциальным и иным сведениям, незаконного извлечения информации или ее уничтожения;

– использование искусственного интеллекта, машинного обучения, нейросистем в целях нанесения вреда;

– распространение медицинских устройств, работающих с беспроводными сетями;

– увеличение количества атак на облачные сервисы (целью атак могут стать сервисы хранения данных, мессенджеры, социальные сети, интернет-проекты хранения данных);

– отсутствие оценки уязвимых узлов государств – членов ОДКБ и их защитных возможностей;

– зависимость информационной безопасности государств – членов ОДКБ от иностранных поставщиков программно-аппаратных компонентов программного обеспечения и оборудования (браузеры, поисковики, социальные сети, операционные системы находятся вне пределов российского контроля);

– нехватка квалифицированных специалистов, программного обеспечения и недостаточная координация с правоохранительными органами;

– несовершенство информационной безопасности в социальной и образовательной сферах, отсутствие элементов кибербезопасности в образовательной системе, как школьной, так и вузовской.

3.3. Некоторые общие недостатки законодательства государств – членов ОДКБ в сфере кибербезопасности:

– неоднозначность терминологии;

– несогласованность между информационно-коммуникационными технологиями (большие данные, облачные технологии, суперкомпьютеры, искусственный интеллект и т. д.) и законодательством государств – членов ОДКБ, регулирующим вопросы безопасности в этой сфере, развития и использования цифровых технологий;

– неоднозначность положений некоторых законов, которые по-разному трактуются государственными регуляторами и операторами, требуют конкретизации, уточнений и разъяснений;

– необходимость адаптации законодательства к глобальным угрозам информационной безопасности на международном уровне, гармонизации и унификации законодательств государств-союзников в условиях формирования глобального информационного пространства и ускоренного роста глобальных угроз информационной безопасности;

– неполноценность уголовных кодексов государств – членов ОДКБ, устанавливающих ответственность за совершение киберпреступлений.

4. Основные направления развития инструментария для противодействия кибервызовам и угрозам

1. Разработка достаточно современной законодательной базы по противодействию кибервызовам и киберугрозам.

2. Выработка правоприменительной политики при имплементации новых подходов и методов противодействия в национальных законодательствах.

3. Обеспечение современных механизмов реализации принимаемых законодательных и нормативных актов в цифровой сфере.

4. Применение действенных мер по распространению своевременной информации, связанной с существующими и появляющимися киберугрозами.

5. Обеспечение надлежащего уровня и перманентное повышение квалификации сотрудников государственных структур, имеющих непосредственное

отношение к цифровой сфере, а также к информационным и другим современным технологиям.

5. Приоритеты противодействия кибервызовам и угрозам:

- совершенствование законодательства государств – членов ОДКБ, способствующего созданию международной нормативно-правовой базы по борьбе с киберугрозами;
- дополнение уголовного законодательства нормами, устанавливающими ответственность за совершение преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем, деяний, связанных с подлогом компьютерных данных. и других противоправных действий, способных причинить тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом. К таким преступлениям можно отнести: незаконный доступ к компьютерной системе или к ее части; умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему; незаконное вмешательство в данные путем умышленного повреждения, стирания, порчи, изменения или подавления компьютерных данных; подлог компьютерных данных, компьютерное мошенничество и т. п.;
- расширение практики привлечения экспертного сообщества, научных и некоммерческих организаций к подготовке ключевых проектов нормативных документов в сфере кибербезопасности;
- упрощение взаимодействия правоохранительных органов с иностранными уполномоченными органами при расследовании инцидентов кибербезопасности;
- подготовка нормативно-правовой базы для совершенствования и применения технологий облачных вычислений, а также разработки и функционирования облачных сервисов;
- принятие необходимых законов и поправок с целью предотвращения следующих угроз:

1) вымогательство путем использования незаконного доступа к компьютерам, мобильным устройствам, аккаунтам в социальных сетях и кабинетам на общедоступных сайтах и т. д.;
2) хулиганство, распространение материалов незаконного характера, подстрекательство, пропаганда насилия, терроризма, экстремизма, призывы к насильственным и иным противоправным действиям;
3) распространение наркотических средств, формул синтетических наркотиков (спайсов) и другой информации по изготовлению различных наркотиков;
4) мошенничество, обманные операции с движимым и недвижимым имуществом, драгоценными металлами и камнями, антиквариатом и т. д.;
5) финансовые пирамиды, отмывание денежных средств, незаконные азартные игры, ложные лотереи, подставные или нереальные брокерские махинации, продажа несуществующих на реальном рынке ценных бумаг и т. д.;
6) фальшивые аукционы, несуществующие в реальной жизни интернет-магазины, ложные благотворительные акции;
7) преследование, незаконный сбор персональных данных и их использование, идентификация лиц;
8) незаконное прослушивание голосовых переговоров или отслеживание и просмотр переписок, а также фото- и видеоматериалов;
9) предложение незаконных или нереальных услуг мошеннического характера;
10) международная, военная, промышленная, деловая, политическая шпионская деятельность;
11) распространение вирусов (вредоносных программ) с целью вредительства либо в рамках одного или нескольких вышеперечисленных пунктов.