

**КИБЕРБЕЗОПАСНОСТЬ И ЕЁ СРАВНИТЕЛЬНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ В
РОССИИ И ЗА РУБЕЖОМ****Слободчикова Анастасия Валерьевна**

студент, ОУ ВО «Южно-Уральский Институт Управления и Экономики», РФ, г. Челябинск

Сотникова Лилия Владимировна

научный руководитель, зав. кафедры «Юриспруденция и гуманитарные науки», ОУ ВО «Южно-Уральский Институт Управления и Экономики», РФ, г. Челябинск

Бурное развитие всего человечества в 21 веке, в основном основано на внедрении новейших компьютерных технологий, а также различных способов доставки какой-либо информации, которые будут протекать во многих сферах нашей общественной жизни, и именно с этого момента человечество всё чаще переходит на новый уровень реальности – глобальной информатизации. Глобальная информатизация динамично управляет существованием и жизнедеятельностью не только жизнью человечества, но и государствами мирового сообщества. В основном это отражается на таких аспектах как обеспечение национальной, военной, экономической, информационной безопасности. Самым глобальным последствием информатизации является киберпространство.

Киберпространство – это транснациональная сфера инфраструктур информационных технологий и взаимосвязанных сетей. Киберпространство состоит из интернета, телекоммуникационных сетей и компьютерных систем.

В киберпространстве, как и в любых других пространствах существуют определённые операции с цифровым кодом, которые направлены на передачу и приём огромного количества информации. Но проводимые операции с использованием цифрового кода, и других вычислительных средств, обычно являются сбором информации о важных системах и ресурсах определённого объекта. Обычно такую деятельность многообразных субъектов в киберпространстве обозначают как кибердеятельность.

В настоящее время все люди имеют различные современные компьютеры, а также выход в глобальную паутину мира, где как отдельные лица, организации, а также государство и его союзники могут выполнять кибердеятельность, для преследования определённых целей, которые неизвестны другим субъектам. Характер этих целей может быть различным, они бывают, как и положительные, так и отрицательные. К положительным обычно относят информирование в целях обучения в различных областях, таких как наука и техника.

А к отрицательным относят, кибердеятельность направленная на достижение нанесения ущерба другому субъекту вне зависимости от его природы. Обычно данная кибердеятельность остаётся безнаказанной. Причинами безнаказанности кибердеятельности может объясняться в следующем:

- Сложность в определении источника воздействия на все информационные ресурсы;
- Сложность в определении местонахождении источника воздействия на информационные ресурсы.

Под кибербезопасностью следует понимать определённый комплекс мероприятий, который направлен на защиту компьютеров, цифровых данных и сетей их передачи, от несанкционированного доступа, и других действий, связанных с:

- Манипулированием
- Блокированием
- Искажением
- Разрушением или уничтожением как умышлено, так и случайным характером.

Во многих различных государствах за последние 10 лет были приняты меры по защите национального киберпространства, где на государственном уровне были разработаны, а также опубликованы стратегии киберпространства. Главным акцентом в стратегиях киберпространства является тем, что «...обеспечение доступности киберпространства, а также целостности, достоверности и конфиденциальности информации в киберпространстве стало одной из важных проблем 21 века. Именно поэтому защита киберпространства становится главной задачей государства, экономики и общества, как на государственном, так и на международном уровне» [4].

В европейских государствах хронология принятия стратегий расположена следующим образом:

- 2008 год – стратегии разработаны, приняты и опубликованы в Словакии, Финляндии и Эстонии.
- 2011 год – к странам, имеющим стратегии по кибербезопасности, присоединились: Германия, Голландия, Литва, Люксембург, Великобритания, Чешская республика, Франция [1].

В них отражено:

- Цели и мероприятия, направленные на развитие оборота электронной информации, а также обеспечения её конфиденциальности, доступности и целостности в кибербезопасности;
- Обеспечение информационной безопасности рассматривается в качестве необходимого условия нормального функционирования и развития общества.

В некоторых из этих стратегиях раскрыты понятия, а также термины, раскрывающие деятельность человечества в киберпространстве, например, в стратегии Литвы говорится о том, что «... для обеспечения безопасности киберпространства необходимо организовывать непрерывно функционирующую и надлежащим образом управляемую систему, контролирующую все стадии управления инцидентами, начиная от раннего предупреждения, предотвращения, обнаружения, устранения, и заканчивая расследованием инцидента» [3].

В голландской стратегии прописано определение кибербезопасности, в котором говорится, что: «Кибербезопасность – это защищённость от сбоев и неправильной эксплуатации информационно-телекоммуникационных систем. Сбои и неправильная эксплуатация может отрицательно повлиять на допустимость и надёжность информационно-телекоммуникационных систем, поставить под угрозу конфиденциальность и целостность информации, хранящейся в системах» [2].

Уникальным на настоящее время международным документом по информационной безопасности является Конвенция по киберпреступлениям, которая принята Советом Европы в 2001 году [5]. Именно эта Конвенция содержит в себе:

- Классификация компьютерных преступлений
- Рекомендации органам законодательной и исполнительной власти государств по борьбе с компьютерными преступлениями.

Но Российская Федерация не ратифицировала Конвенцию по киберпреступлениям, где она содержала свою позицию и выразила её в документе «Принципы, касающиеся международной информационной безопасности». Данный документ был представлен на рассмотрении Генеральной Ассамблеи ООН.

Так же в этом документе говорилось, об развитии военного потенциала отдельных стран за счёт применения новейших информационных технологий, которые ведут к переменам

глобального и регионального баланса сил. По мнению Российской Федерации, представляется потребность в международно-правовом регулировании мировых процессов не только со стороны гражданской информатизации, но также и с военной.

Позиция США в отличии от Российской Федерации, основывается на том, что наиболее главной потребностью является разработка мер информационной безопасности применительно к угрозам террористического и криминального характера.

Исходя из всего этого, можно сделать вывод о том, что Европа сделала акцент на разработке Конвенции по киберпреступлениям, а США не стремится к достижению международной договорённости по урегулированию террористических угроз. Следовательно, Российская Федерация, остаётся без поддержки своей позиции на мировом политическом пространстве.

На данный момент в СМИ Российской Федерации обсуждается совершенно новый проект «Концепции стратегии кибербезопасности» [6]. Данный проект будет содержать в себе нормативно-правовую базу, которая будет осуществлять не только деятельность кибербезопасности, но и проводить правовой контроль за этой деятельностью.

Список литературы:

1. Государственные стратегии кибербезопасности [Электронный ресурс]. - Режим доступа: <https://www.securitylab.ru/analytics/429498.php> (дата обращения 11.10.2018) [1].
2. The National Cyber Security Strategy (NCSS) [Электронный ресурс]. - Режим доступа: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf> (дата обращения 11.10.2018) [2].
3. Government of the republic of Lithuania. Resolution № 796 of 29 June 2011 [Электронный ресурс]. - Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (дата обращения 11.10.2018) [3].
4. Cyber Security Strategy for Germany [Электронный ресурс]. - Режим доступа: <https://studylib.net/doc/12953062/cyber-security-strategy-for-germany> (дата обращения 11.10.2018) [4].
5. Конвенция по киберпреступлениям [Электронный ресурс]. - Режим доступа: <http://base.garant.ru/4089723/> (дата обращения 11.10.2018) [5].
6. Концепция стратегии кибербезопасности российской федерации [Электронный ресурс]. - Режим доступа: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf> (дата обращения 11.10.2018) [6].