Статья 10

Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу на 30-й день с даты получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

2. Стороны могут вносить в настоящее Соглашение изменения, которые по взаимному согласию Сторон оформляются отдельным протоколом.

3. Действие настоящего Соглашения может быть прекращено по истечении 90 дней с даты получения одной из Сторон по дипломатическим каналам письменного уведомления другой Стороны о ее намерении прекратить действие настоящего Соглашения.

4. В случае прекращения действия настоящего Соглашения Стороны принимают меры для полного выполнения обязательств по защите информации, а также обеспечивают выполнение ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках настоящего Соглашения и не завершенных к моменту прекращения действия настоящего Соглашения.

Совершено в г. " " 20 г. в двух подлинных экземплярах на русском языке.

За Правительство
Российской Федерации

За Правительство
Республики Беларусь

_____

ПРИЛОЖЕНИЕ № 1
к Соглашению между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности

ПЕРЕЧЕНЬ
основных понятий в области обеспечения международной информационной безопасности

"Информационная безопасность" - состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

"Информационная война" - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим объектам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

"Информационная инфраструктура" - совокупность технических средств и систем создания, преобразования, передачи, использования и хранения информации.

"Информационное оружие" - информационные технологии, средства и методы, применяемые в целях ведения информационной войны.

"Информационная преступность" - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях.

"Информационное пространство" - сфера деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

"Информационные ресурсы" - информационная инфраструктура, а также собственно информация и ее потоки.
"Информационный терроризм" - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях.
"Защита информации" - комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации.
"Критически важные объекты" - объекты инфраструктуры государства, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики государства либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок.
"Международная информационная безопасность" - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.
"Неправомерное использование информационных ресурсов" - использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств каждой из Сторон либо норм международного права.
"Несанкционированное вмешательство в информационные ресурсы" - неправомерное воздействие на процессы создания, обработки, преобразования, передачи, использования, хранения информации.
"Угроза информационной безопасности" - факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.

_____

ПРИЛОЖЕНИЕ № 2
к Соглашению между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности
ПЕРЕЧЕНЬ
основных угроз в области международной информационной безопасности, их источников и признаков
1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.
Источник угрозы - создание и развитие информационного оружия, способного нанести ущерб критически важным объектам государств, что может привести к новой гонке вооружений.
Признаки угрозы - применение информационного оружия в целях подготовки и ведения информационной войны, воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные объекты.
2. Информационный терроризм.
Источник угрозы - террористические организации и лица, причастные к террористической деятельности, осуществляющие противоправные действия посредством или в отношении информационных ресурсов.
Признаки угрозы - использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации;

использование сети "Интернет" или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе; иное негативное воздействие на информационные ресурсы.
3. Информационная преступность.
Источник угрозы - лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.
Признаки угрозы - проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление сетевых атак и иного негативного воздействия; причинение ущерба информационным ресурсам; нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни; использование информационных ресурсов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т. д.
4. Использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств.
Источник угрозы - неравномерность в развитии информационных технологий в различных государствах и существующая тенденция к увеличению "цифрового разрыва" между развитыми и развивающимися странами. Некоторые государства, имеющие преимущества в развитии информационных технологий, умышленно ограничивают развитие прочих стран и получение доступа к информационным технологиям, что приводит к возникновению серьезной опасности для государств с недостаточными информационными возможностями.
Признаки угрозы - монополизация производства программного обеспечения и оборудования информационных инфраструктур, ограничение участия государств в международном информационно-технологическом сотрудничестве, препятствующее их развитию и увеличивающее зависимость этих стран от более развитых государств; встраивание скрытых возможностей и функций в программное обеспечение и оборудование, поставляемые в другие страны, для контроля и влияния на информационные ресурсы и (или) критически важные объекты этих стран; контроль и монополизация рынка информационных технологий и продуктов в ущерб интересам и безопасности государств.
5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.
Источники угрозы - государства, организации, группа лиц или частные лица, использующие информационную инфраструктуру для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.
Признаки угрозы - появление и тиражирование в электронных (радио и телевидение) и прочих средствах массовой информации, в сети "Интернет" и других сетях информационного обмена информации:
искажающей представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения;
пропагандирующей идеи терроризма, сепаратизма и экстремизма;
разжигающей межнациональную, межрасовую и межконфессиональную вражду.
6. Угрозы безопасному и стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.
Источники угроз - стихийные бедствия и другие опасные природные явления, а также катастрофы

техногенного характера, способные оказать масштабное разрушительное воздействие на информационные ресурсы государства.
Признаки угроз - нарушение функционирования объектов информационной инфраструктуры и, следовательно, дестабилизация критически важных объектов, государственных систем управления и принятия решений, результаты которой прямо затрагивают безопасность государства и общества.

_____