Информационная безопасность
государства и личности

СЕКТОР
ИНФОРМАЦИЯ и КИБЕРБЕЗОПАСНОСТЬ (ФАМИ)

Информационная безопасность

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Основные цели информационной безопасности

Конфиденциальность

Доступность

Подлинность

Целостность

Конфиденциальность

Конфиденциальность – это состояние доступности информации только авторизованным пользователям, процессам и устройствам.

Чтобы обеспечить конфиденциальность информации, её нужно

- Закрыть (разграничить доступ)
- Скрыть (сделать неизвестным сам факт существования информации)
- Зашифровать
- Разделить на части

Целостность

Целостность – это отсутствие неправомочных искажений, добавлений или уничтожения информации. Гарантия целостности особенно важна в тех случаях, когда информация представляет большую ценность и не должна быть потеряна, а также когда данные могут быть намеренно изменены в целях дезинформации получателя. Как правило, от стирания информацию защищают методами, обеспечивающими конфиденциальность, и резервным копированием, а отсутствие искажений проверяют с помощью хеширования.

Доступность

Доступность – это обеспечение своевременного и надежного доступа к информации и информационным сервисам. Типичными случаями нарушения доступности являются сбой в работе программных/аппаратных средств и распределенная атака типа «отказ в обслуживании» (DDoS). От сбоев информационную систему защищают устранением причин сбоев, а от DDoS-атак – отсечением паразитного трафика.

Подлинность или аутентичность

Подлинность или аутентичность – возможность однозначно идентифицировать автора/источник информации. Подлинность электронных данных часто удостоверяется таким средством, как электронно-цифровая подпись.

Неотказуемость*

Неотказуемость – неотрекаемость от авторства информации, а также факта её отправки или получения. Неотказуемость можно гарантировать электронно-цифровой подписью и другими криптографическими средствами и протоколами. Неотказуемость актуальна, например, в системах электронных торгов, где она обеспечивает ответственность друг перед другом продавцов и покупателей.

Информационная безопасность государства

Для государства все цели ИБ приобретают категорическую значимость. В условиях информационного общества информация – это, прежде всего, стратегический ресурс, определяющий функционирование любой сферы общества. Данный стратегический ресурс дифференцирован по разным социальным сферам.

Экономическая сфера

Характерной чертой современной экономики является не только уровень фактического производства (выработка n-го количества товара), сколько престиж государственной экономики на мировой арене, доверие к экономическим институтам внутри страны и их влияние на институты экономики вовне. Своего рода маркетинг, объектом которого выступает не какой-либо продукт, а государство, точнее государственная экономика или бренд, «made in…».

Сфера международной политики

Современные международные отношения от физического (вооруженного) противостояния перешли в разряд информационной борьбы, где главенствующую роль приобретает дипломатия и СМИ. Символично это можно представить таким образом: решение международных конфликтов преимущественно переместилось от поля боя в кабинеты.

Сфера внутренней политики

Так, основным способом легитимации власти преобладающего большинства развитых стран является ее выборность. Именно процедура избрания, с ее рейтингами отдельных лидеров или политических партий – плацдарм для информационной борьбы в чистом виде. Где информация различного толка способна как «похоронить» политическую карьеру, так и возвести на «пьедестал».

Оборонная сфера

Оборонная сфера, став высокотехнологичным потребителем научной отрасли, также напрямую зависит от контроля за информационными потоками. Доступ (как физический, так и информационный) к новинкам из области «hi-tech» и другим составляющим оборонной промышленности должен быть строго ограничен, так как это представляет вопрос национальной безопасности. Оборонная отрасль зачастую используется как гарант экономической состоятельности государства и как опора при ведении политики на различных уровнях.

Информационная безопасность личности

Помимо физических и психических особенностей, свойственных любому индивиду, личность приобретает и виртуальную характеристику, представляющую собой разнородную информацию о какой-либо персоне. Оперирование данной персональной информацией становится социально значимой потребностью для граждан информационного общества.

Информационная безопасность личности

Информационное поле предоставляет исчерпывающую информацию об индивиде: это и сфера деятельности, профессия, друзья, область интересов, хобби и т.д. Помимо этого могут быть зафиксированы отдельные факты биографии, фото- и видеоматериалы с участием индивида, высказывания. в том числе и касательно социально-экономических и политических вопросов, на основании которых можно составить ценностную модель и выявить основополагающие поведенческие установки.

Информационная безопасность личности

Также в информационном массиве зачастую содержатся конфиденциальные данные: место жительства, контактные телефоны, номера банковских счетов и пластиковых карт, паспортные данные и тому подобное. Таким образом, персональная сопряженность с информационным полем и даже зависимость от него характерны для любой личности, социализированной посредством культуры общества информационной эпохи.

Информационная безопасность государства и личности

Если информационная безопасность в глобальном масштабе и на уровне отдельных государств представляет собой предмет профессиональной работы специализированных управлений и ведомств, то личная информационная безопасность - это перспективное направление будущего. Данная сфера деятельности теоретически должна будет предоставлять целый спектр услуг, наподобие «создания благоприятного личного образа в информационном поле» или «зачистки персонального имиджа от порочащих фактов биографии».

Резюмируя, необходимо обратить особое внимание на три аспекта исследуемой проблемы:

- **Во-первых,** на тот факт, что информация (особенно дезинформация) является мощным оружием, которая зачастую используется латентными силами для осуществления культурной десуверенизации, смены политических элит и политического курса в конкретном государстве.
- **Во-вторых,** основным источником распространения деструктивной информации становятся, как правило, Интернет и социальные сети, что необходимо регламентировать с помощью политико-правового механизма.
- **В-третьих,** в качестве инструмента для смены политического строя и политических элит, как доказывает практика, информационными агрессорами используются массовые мероприятия, которые при определенной подготовке, информационном воздействии перерастают в массовые беспорядки, сопровождающиеся погромами и физическим насилием.

С целью недопущения деструктивных проявлений информации необходимо обеспечить своевременное реагирование на всех уровнях на выявленные деструктивные аспекты, которые касаются, прежде всего, разработки более адекватного для информационного общества политико-правового механизма и правового поля. С этой целью в Республике Беларусь принят ряд законодательных актов (Закон Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации», Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Постановление Совета Министров Республики Беларусь «Об утверждении Положения о порядке предварительной идентификации пользователей интернет-ресурса, сетевого издания»), которые определяют порядок распространения информации в СМИ, в сети Интернет и т.д.

СЕКТОР
ИНФОРМАЦИЯ и КИБЕРБЕЗОПАСНОСТЬ (ФАМИ)

г.Гродно, ул.Ожешко 22, ауд.222, тел. +375-152-72-13-92
e-mail: kaf_spkb@grsu.by