

ЭКСПЕРТНО-КОНСУЛЬТАТИВНЫЙ СОВЕТ  
ПРИ СОВЕТЕ ПАРЛАМЕНТСКОЙ АССАМБЛЕИ  
ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ

---



*Санкт-Петербургский институт  
информатики и автоматизации  
Российской академии наук*

# СЛОВАРЬ – СПРАВОЧНИК

## ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПАРЛАМЕНТСКОЙ АССАМБЛЕИ ОДКБ

Санкт-Петербург  
2014



**ЭКСПЕРТНО-КОНСУЛЬТАТИВНЫЙ СОВЕТ ПРИ СОВЕТЕ  
ПАРЛАМЕНТСКОЙ АССАМБЛЕИ  
ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ**

---

*Управление ФСТЭК России  
по Северо-Западному федеральному округу  
Санкт-Петербургский институт информатики и автоматизации РАН*

**СЛОВАРЬ – СПРАВОЧНИК  
ПО ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ  
ДЛЯ ПАРЛАМЕНТСКОЙ АССАМБЛЕИ  
ОДКБ**

Санкт-Петербург  
2014

УДК 004  
ББК 92; Я2

*Рекомендовано к публикации кафедрами международной и национальной безопасности  
Северо-Западного института РАНХ и ГС  
при Президенте Российской Федерации (протокол от 03.06.2014)*

*Рецензент – д.ю.н. Бачило И.Л. (ИГП РАН)*

*Коллектив составителей:  
Вус М.А., Кучерявый М.М., Подкидышева В.Е.,  
Шакин Д.Н., Юсупов Р.М.*

**СЛОВАРЬ – СПРАВОЧНИК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПАРЛАМЕНТСКОЙ АССАМБЛЕИ ОДКБ** / Под общ. ред. М.А. Вуса и М.М. Кучерявого. – СПб.: СПИИРАН. Изд-во «Анатолия». «Полиграфические технологии», 2014. – 96 с.

**ISBN 978-5-7452-0050-2**

Издание адресовано парламентариям, членам экспертных групп и комиссий, работникам органов СНГ и рабочих органов Межпарламентской Ассамблеи СНГ, Парламентской Ассамблеи ОДКБ и иных интеграционных объединений государств постсоветского пространства. Справочный материал может быть использован в правотворческой и правоприменительной деятельности, в научных исследованиях и в учебном процессе.

**ISBN 978-5-7452-0050-2**

© Коллектив авторов, 2014  
© СПИИРАН, 2014  
© Изд-во «Анатолия», 2014

## СОДЕРЖАНИЕ

Предисловие .....	4
<b>АБРИС ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .....</b>	<b>6</b>
Литература .....	11
<b>ЭСКИЗ СИСТЕМНОГО ПОДХОДА К ФОРМИРОВАНИЮ ПОНЯТИЙНОГО АППАРАТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .....</b>	<b>12</b>
Литература .....	34
<b>ПОНЯТИЙНЫЙ АППАРАТ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИЗ НОРМАТИВНЫХ АКТОВ ГОСУДАРСТВ – ЧЛЕНОВ ОДКБ .....</b>	<b>36</b>
Перечень нормативных источников, использованных при составлении Словаря-справочника .....	86
<b>АЛФАВИТНЫЙ УКАЗАТЕЛЬ .....</b>	<b>88</b>
<i>Книжная полка .....</i>	<i>93-95</i>

## ПРЕДИСЛОВИЕ

Организация Договора о коллективной безопасности (ОДКБ) — международная организация военно-технического сотрудничества, созданная на постсоветском пространстве, объединяет в настоящее время шесть независимых государств: Республику Армения, Республику Беларусь, Республику Казахстан, Кыргызскую Республику, Российскую Федерацию и Республику Таджикистан. ОДКБ позиционирует себя как многофункциональная структура противодействия традиционным и новым вызовам и угрозам миру, безопасности и стабильности. Диапазон таких вызовов в последнее время не только не сужается, а, напротив, расширяется. Учитывая это обстоятельство, Президент Российской Федерации В.В. Путин особо подчеркнул, что *«совместно с нашими союзниками мы должны укреплять возможности Организации Договора о коллективной безопасности»*.

В качестве одного из основных направлений создания системы коллективной безопасности государства – члены ОДКБ рассматривают сближение основных положений законодательных актов в области обороны и безопасности. Парламентская Ассамблея Организации Договора о коллективной безопасности (ПА ОДКБ) является органом межпарламентского сотрудничества государств – членов ОДКБ, созданным в рамках Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств (МПА СНГ). ПА ОДКБ обсуждает вопросы сотрудничества государств – членов, принимает рекомендации по сближению законодательства этих государств в международной, военно-политической, гуманитарной и иных областях. Рабочим языком Парламентской Ассамблеи является русский язык.

Важнейшим компонентом национальной и международной безопасности становится сегодня информационная безопасность. Информационные технологии стали одним из важнейших политико-экономических и военных ресурсов, повсеместно растут техногенные факторы и связанная с этим уязвимость. Информационная сфера — весьма чувствительный фактор жизнедеятельности общества, глобализация информационных процессов повлекла за собой возникновение целого спектра проблем безопасности. Само понятие информационная безопасность превратилось из узкотехнического в широкоупотребительное.

Совместная деятельность государств – членов ОДКБ в сфере обеспечения информационной безопасности преследует своей целью более эффективную защиту их законных интересов в информационном пространстве. В формате ОДКБ существует согласие относительно того, что под информационной безопасностью понимается ***состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.***

Программа совместных действий государств – членов ОДКБ по формированию системы информационной безопасности была принята в 2008 г.; обеспечение информационной безопасности как важное направление сотрудничества в 2010 г. закреплено в Уставе Организации. В этой связи особую актуальность приобрели вопросы формирования активной согласованной информационной политики государств по развитию общего информационного пространства, создания совместного потенциала по противодействию информационным угрозам правам и свободам граждан и интересам государства и общества, защищенности информационных ресурсов и коммуникаций органов ОДКБ, национальных органов власти и управления.

Согласованная политика требует определенности и однозначности понятийного аппарата. Массив понятий и дефиниций, обслуживающих сферу информатики, начал формироваться сравнительно недавно. Понятийный аппарат, складывающийся в разных отраслях законодательства, обусловлен характером регулируемых отношений. При этом юридические определения многочисленных специальных терминов зачастую играют решающую роль при толковании норм законов в правоприменительной практике. В силу этого в области юрисдикции государств – членов ОДКБ как во внутригосударственной сфере, так и в международном пространстве большую роль играет выбор конкретных значений применяемых терминов и понятий, их легитимное толкование и применение в различных договорах, соглашениях и иных актах, прежде всего, в актах имеющих политическое, экономическое и юридическое значение.

За два десятилетия существования Независимых Государств на постсоветском пространстве разработано и принято большое число нормативно-правовых актов, однако для большинства этих актов сегодня характерны терминологическое многообразие и слабая определенность используемого понятийного аппарата. В этой связи необходима унификация в нормативно-правовой базе государств – членов ОДКБ, прежде всего, базовых терминов и понятий, используемых в процессе нормативного правового регулирования и сотрудничества в области обеспечения информационной безопасности, их единообразная трактовка.

Предлагаемый справочник содержит 163 группы терминов и различных трактовок понятий, относящиеся к сфере информационной безопасности. Словарный материал представлен в табличной форме. Он включает набор категорий, которые можно рассматривать как базовые для сферы информационной безопасности, а также относящиеся к сфере информационной безопасности лексические единицы, получившие юридическое толкование в международных и национальных правовых документах государств – членов ОДКБ, с указанием их первоисточника. Представленная выборка понятийного аппарата не претендует на полноту, но может послужить ориентиром в правотворческой деятельности.

**М.А. Вус**

*кандидат технических наук,  
СПИИРАН*

**М.М. Кучерявый**

*кандидат политических наук,  
ФСТЭК России*

## **АБРИС ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<sup>1</sup>**

Важнейшим результатом формирования информационного общества на рубеже XX-XXI веков стало возникновение глобального информационного пространства, в котором развернулась острая борьба за достижение информационного превосходства. Вследствие этого в современном обществе информационная безопасность является важнейшим компонентом национальной, региональной и международной безопасности.[1]

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. На современном этапе социального развития информация и информационные ресурсы стали одним из решающих факторов развития личности, общества и государства. Идёт активная разработка и внедрение во все сферы человеческой деятельности информационных и информационно-телекоммуникационных технологий (ИКТ). Доступность информационных услуг и ИКТ приобрела непосредственную социальную значимость, вошла в число параметров, характеризующих качество жизни современного человека, реализацию его основных прав и свобод. Однако существенным препятствием для полномасштабного использования потенциала современных ИКТ в достижении устойчивого развития мирового сообщества является возрастание угроз военно-политического, террористического и криминального характера, всё сильнее проявляющееся в информационной сфере.

Информация и ИКТ всё чаще начинают использоваться в качестве определённых угроз интересам конкурентов. Всё явственнее проявляется стремление различных субъектов (коалиций, государств, организаций, личностей) к единоличному обладанию информационными ресурсами, средствами и технологиями, и их использованию в целях удовлетворения собственных интересов и противодействия интересам вероятных конкурентов в экономическом, коммерческом и даже военном противоборстве. По существу это обстоятельство и породило проблему информационной безопасности.[2,3]

Концептуальные и научно-методологические основы информационной безопасности ещё только начинают разрабатываться. В центре внимания исследователей и разработчиков находятся как вопросы структуризации самой проблемы информационной безопасности и классификации источников информационных угроз, критерии и нормативы информационной безопасности, так и уточнение терминологии этой предметной области, её и легитимация и легализация. Термин «обеспечение информационной безопасности» получил распространение в литературе по политологии, психологии, техническим и юридическим наукам, вместе с тем к трактовке самого понятия «информационная безопасность» имеют место различные подходы.

К первоочередным задачам при создании теории информационной безопасности относится формирование системы базовых понятий, среди которых

---

1 **Абрис** (нем.) – очертание предмета, контур, рисунок в общих чертах.

«информационная опасность», «информационная угроза», «информационная безопасность» и др. В литературе в настоящее время присутствует множество трактовок таких понятий. На уровне обыденного сознания понятие «безопасность» определяется как отсутствие опасности. Содержание категории безопасность традиционно раскрывается через такие понятия как «объекты безопасности», «угрозы безопасности», «виды безопасности» и др.[3]

Необходимость максимально строго придерживаться в сфере безопасности легальных терминов вытекает из потребности формализации управленческих решений, регламентации прав и ответственности. Такая терминология должна использоваться различными коллективами (и не только исследователей и технических специалистов, но и функционеров: чиновников, политиков, менеджеров), работающими в разных предметных областях и решающими на практике сложные и многоаспектные проблемы безопасности. Неоднозначная и противоречивая трактовка основополагающих понятий в сфере, связанной с проблемами безопасности, не допустима, это может повлечь далеко идущие негативные последствия.

В определениях, используемых многими специалистами, безопасность рассматривается как одна из сторон защищенности. Так, например, в Доктрине информационной безопасности Российской Федерации безопасность определяется как *«состояние защищенности жизненно важных интересов граждан, общества и государства в информационной сфере»*. Ключевыми словами в данном определении являются: информационная безопасность, защищенность, жизненно важные интересы, информационная сфера. Но безопасность не всегда обеспечивается только защитой. Она может быть достигнута также соответствующими правилами поведения и взаимодействия объектов, высокой профессиональной подготовкой персонала, безотказностью работы техники, надёжностью всех видов обеспечения функционирования объектов безопасности и т.д.[3]

В настоящее время имеет место распространённый на практике подход, когда понятие информационная безопасность изначально сужается и рассматривается только в его технико-технологическом срезе (как это принято в специальной англоязычной литературе). Так, например, авторы Глоссария по информационному обществу [4] приводят понятие «информационная безопасность – Information security» в следующей трактовке:

1. Защищенность информации от возможных угроз, направленных на нарушение её конфиденциальности, целостности, доступности или на её умышленное искажение.

2. Система мер, методов и средств правового, организационного и технологического характера, обеспечивающих предотвращение умышленного или случайного нарушения конфиденциальности, целостности, доступности и искажения информации.

Очевидно, что здесь изначально более широкое понятие «информационная безопасность» подаётся только лишь как «безопасность информации».

Доктрина информационной безопасности Российской Федерации — документ политический, определения в ней носят, в известной мере, характер деклараций. В научном плане определения должны формулироваться как можно более строго и четко определять границы области, задаваемой формируемым определением. В монографии Санкт-Петербургских ученых [5] предпринята по-

пытка с учётом семантики понятий опасность, безопасность и угроза дать такие определения базовым понятиям теории информационной безопасности.

**Информационная опасность** — это:

- состояние окружающей среды или объекта, в котором существует потенциальная возможность причинить объекту существенный ущерб или вред путём оказания воздействия на информационную сферу объекта;

- свойство объекта, характеризующее его способность наносить существенный вред какому-либо объекту путём оказания воздействия на информационную сферу этого объекта.

**Информационная угроза** — угроза объекту путём оказания воздействия на информационную сферу, т.е.:

- намерение нанести (причинить) объекту существенный ущерб путём оказания воздействия на его информационную сферу;

- информационная опасность, реализация которой становится весьма вероятной;

- фактор или совокупность факторов, создающих информационную опасность объекту. Такими факторами могут быть действия, поведение объектов, природные явления и т.д.

**Информационная безопасность** — это:

- состояние объекта, когда ему путём воздействия на его информационную сферу не может быть нанесён существенный ущерб или вред;

- свойство объекта, характеризующее его способность не наносить существенного ущерба какому-либо объекту путём оказания воздействия на информационную сферу этого объекта.

На базе приведенных определений понятие информационной безопасности государства, по мнению авторов, может быть сформулировано как состояние страны, в котором гражданам, объединениям и общественным группам граждан, обществу и государству не может быть нанесён существенный ущерб путём оказания воздействия на информационную сферу страны. Основными объектами информационной безопасности при этом являются личность (её права и свободы), общество (его материальные и духовные ценности) и государство (его конституционный строй, суверенитет, территориальная целостность, экономика, военное дело и т.д.).

**Информационная безопасность личности** — это состояние человека, в котором его личности не может быть нанесён существенный ущерб путём оказания воздействия на окружающее человека информационное пространство.

**Информационная безопасность общества** — это состояние общества, в котором ему не может быть нанесён существенный ущерб путём воздействия на информационную сферу общества.

Основу информационной безопасности общества составляет безопасность индивидуального, группового и массового сознания граждан при наличии информационных угроз, к которым в первую очередь следует отнести информационно-психологические воздействия. Действие этих угроз может вызвать психоэмоциональную и социально-психологическую напряженность, искажение нравственных критериев и норм, морально-политическую дезориентацию и, как следствие, не-

адекватное поведение отдельных лиц, групп и масс людей. В результате таких воздействий возможны глубокие трансформации индивидуального, группового и массового сознания, негативные изменения морально-политического и социально-психологического климата в обществе.

**Информационная безопасность государства** — это состояние государства, в котором ему не может быть нанесён существенный ущерб путём оказания воздействия на информационную сферу государства.[6]

В информационной сфере наибольшее внимание привлекают к себе две опасности. Первая — контроль (извлечение) информационных ресурсов государства, т.е. фактически информационная разведка (шпионаж). Информационное пространство было и остаётся сферой деятельности многочисленных разведывательных служб. Вторая опасность — угроза разрушения или дезорганизации информационных ресурсов элементов государственных структур. При современном уровне развития информационных технологий такие воздействия могут осуществляться и в мирное время. Эти воздействия могут привести или к разрушению ценной для государства информации или к её искажению, или к внедрению негативной информации в целях дезорганизации или принятия неправильных решений на соответствующем уровне государственного управления.

Безопасность во многом зависит от защищенности так называемых критических инфраструктур, вывод из строя которых приводит к развалу системы безопасности. К критическим инфраструктурам в информационной сфере сегодня относят, прежде всего, компьютерные системы управления, базы данных и т.п. Наряду с этим Аналитическая Ассоциация ОДКБ, не без оснований, предлагает ввести в обиход также понятие о критических инфраструктурах духовно-нравственного контента и информационного пространства стран ОДКБ.[7]

Проблема информационной безопасности породила в последние годы такие понятия как «информационное противоборство», «информационная война (борьба)», «информационное оружие», «информационный терроризм» и др. Бурное развитие и применение ИКТ и, как следствие, формирование новой пространственной структуры — информационной сферы (пространства) инициировали рождение принципиально новой составляющей современной геополитики — информационной геополитики. Такая геополитика уже сегодня активно развивается в США в форме стратегического информационного превосходства (преобладания) и доминирования.

**Информационная война** — это действия, предпринимаемые для достижения информационного превосходства путём нанесения ущерба информационной сфере противника и обеспечения собственной информационной безопасности. Угроза информационной войны в глобальном контексте есть фактор скрытого военно-политического давления и запугивания — фактор, способный нарушить стратегический паритет, подорвать сложившееся равновесие на мировой политической арене.

Информационные войны ведутся с помощью информационного оружия, применение которого по эффективности сравнимо с действием оружия массового поражения. Кроме того, информационное оружие может активно применяться и в мирное время. Американские военные, например, всё больше фокусируются на развитии ударных возможностей в информационном пространстве. По оцен-

кам аналитиков, только в 2011 году спецслужбы США совершили свыше двухсот наступательных киберопераций, три четверти из которых были направлены против Ирана, России, Китая и Северной Кореи [8].

В условиях массовой информатизации немалую опасность представляет ширящийся информационный криминал — действия отдельных лиц или групп, направленные на нанесение ущерба информационной сфере или её использование в корыстных целях. Развитие и доступность информационных технологий влечёт за собой необходимость совершенствования защиты информации и выработки новых стратегий борьбы с преступностью. Важным геополитическим фактором стала сегодня угроза информационного терроризма, борьба с которой требует объединения усилий всех государственных институтов и активизации международного сотрудничества.

Порождаемые информатизацией проблемы информационной безопасности являются глобальными, они затрагивают все государства и их региональные организации. Без подключения к мировому информационному пространству страны и народы обречены на экономическое прозябание, а участие государств в международных системах телекоммуникаций и информационного обмена невозможно без комплексного решения проблем информационной безопасности.

В 2009 году в рамках Шанхайской организации сотрудничества было подписано межправительственное Соглашение в области обеспечения международной информационной безопасности (МИБ), которое два года спустя вступило в силу. Соглашение определяет основные угрозы в области обеспечения международной информационной безопасности, направления и принципы сотрудничества, а также формы и механизмы осуществления взаимодействия в сфере МИБ. Разоблачения противоправной деятельности с использованием ИКТ, поразившие мир в последнее время, подтверждают своевременность, значимость и необходимость продвижения инициативы России и её союзников, государств – членов ОДКБ по сопряжению усилий международного сообщества в укреплении МИБ в рамках региональных и международных организаций под эгидой ООН.[9]

Интересы международного сотрудничества требуют обеспечения совместимости национальных векторов информационного развития и приоритетных направлений обеспечения информационной безопасности. В качестве одного из основных направлений создания системы коллективной безопасности государства – члены ОДКБ рассматривают сближение основных положений законодательных актов в области обороны и безопасности.

Для эффективного взаимодействия и сотрудничества необходима развитая система терминов и понятий, их определений, её закрепление в нормативных актах и общественном обращении, а также правовое толкование понятийного аппарата в повседневной практике. От единого понимания правовых подходов к формированию системы информационной безопасности сегодня зависит развитие системы обеспечения как международной и коллективной, так и национальной безопасности государств.

За время, прошедшее после заключения Договора о коллективной безопасности, в ОДКБ разработана правовая база, регламентирующая деятельность этой Организации, принято большое число международных и национальных правовых актов. Однако большинство существующих сегодня нормативных актов в

информационной сфере характеризуют терминологическое многообразие и слабая определенность понятийного аппарата.

Согласование политик требует определенности и однозначности используемого понятийного аппарата. Политикам, органам власти и управления, субъектам хозяйственной деятельности, физическим и юридическим лицам необходимы сведения, основанные на едином понимании предметов и явлений информационного пространства, регулируемого законодательными положениями. С учётом сказанного необходима унификация в нормативно-правовой базе государств – членов ОДКБ, прежде всего, базовых терминов и понятий, используемых в процессе нормативно правового регулирования и сотрудничества в области обеспечения информационной безопасности, проработка их единообразных трактовок.[10]

### **Литература:**

1. История информатики и философия информационной реальности / Под ред. Р.М. Юсупова и В.П. Котенко. – М.: Академический проект, 2007.
2. **Вус М.А., Гусев В.С., Долгирев Д.В., Молдовян А.А.** Информатика: Введение в информационную безопасность. – СПб.: Изд-во «Юридический центр Пресс», 2004.
3. **Юсупов Р.М.** Наука и национальная безопасность 2-е издание. – СПб.: Наука, 2011.
4. Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. – М.: Институт развития информационного общества, 2009.
5. **Юсупов Р.М., Заболотский В.П.** Концептуальные и научно-методологические основы информатизации. – СПб.: Наука, 2009.
6. **Заболотский В.П., Кучерявый М.М.** Проблема информационной безопасности и развитие информационного общества // Информатизация и связь 2012, № 9. С. 3-6.
7. Публичный доклад Аналитической Ассоциации ОДКБ. – М., ОДКБ, 2013.
8. **Смирнов А.А.** «Snowdendate»: анализ цифрового фашизма спецслужб США и их союзников // Информационная безопасность России. Аналитический сборник. Выпуск 1. – М.: Инфофорум, 2014. С. 105-120.
9. Международная информационная безопасность: Проблемы и решения / Под общей ред. С.А. Комова. – М., 2011.
10. **Шушин В.О.** О состоянии и перспективах сотрудничества государств – членов ОДКБ по формированию системы информационной безопасности // Законодательство государств – членов ОДКБ в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации. Материалы международной научно-практической конференции (Санкт-Петербург, 28.11.2013). – СПб.: Секретариат Совета МПА СНГ, 2014. С. 4-10.

*Верно определяйте слова,  
и вы освободите мир  
от половины недоразумений*

Рене Декарт

## **ЭСКИЗ СИСТЕМНОГО ПОДХОДА К ФОРМИРОВАНИЮ ПОНЯТИЙНОГО АППАРАТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<sup>2</sup>**

Системность явлений реального мира не вызывает сомнений. Правилom современного научного исследования стало рассмотрение объектов, предметов, процессов и явлений с точки зрения системного подхода, т.е. комплексно, многоаспектно, во всей совокупности составляющих их элементов, связей и отношений. Системный подход дает возможность рассматривать любую организацию как единое целое, с целью достижения наибольшей эффективности функционирования всей системы, несмотря на возможное наличие у ее элементов противоречивых стремлений [1,2]. Это утверждение в полной мере относится и к такой специфической предметной области теории и практики, как информационная безопасность [3].

С началом становления глобального информационного общества резко увеличилось число комплексных проблем информационной безопасности, требующих участия в их решении специалистов различных областей знаний. Научные направления, занимающиеся исследованием проблем информационной безопасности, развиваясь на различной прикладной и теоретической основе, использовали сходные понятия, но трактовали их неоднозначно. Объективно возникла необходимость системного представления современной терминологии информационной безопасности с учетом исторического опыта, современных реалий и результатов научного прогнозирования развития данной области знаний.

По мнению авторов, основные понятия, определения и термины информационной безопасности могут быть объединены в три группы:

- I. Термины, определяющие научную основу информационной безопасности.
- II. Термины, определяющие предметную область информационной безопасности.
- III. Термины, определяющие основы деятельности по обеспечению информационной безопасности.

Важно подчеркнуть, что расположение терминов в каждой группе определяется не просто алфавитным порядком, а принципом: определение предыдущего термина должно способствовать пониманию каждого последующего термина. Такой подход, по мнению авторов, должен позволить в последующем расширять и дополнять массив терминов.

---

<sup>2</sup> Прагматический взгляд авторов, впервые опубликованный в журнале «Информатизация и связь». 2012, № 9.

## I. ТЕРМИНЫ, ОПРЕДЕЛЯЮЩИЕ НАУЧНУЮ ОСНОВУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К первой группе отнесены термины, во-первых, используемые во многих областях знаний, и, во-вторых, являющиеся однозначными, семантически унифицированными и стилистически нейтральными. Термины этой группы отвечают требованиям однозначности и устойчивости, т.е. эти термины однозначно употребляются в одной области знаний и сохраняют свой особый смысл в каждой другой области знаний, а также являются общепризнанными — они употребляются в обиходе. Это, прежде всего, такие термины как «информация».

Информация проникает во все сферы и направления деятельности человека, общества и государства. От качества и достоверности информации, оперативности ее получения зависят многие решения, принимаемые на самых разных уровнях — от главы государства и до отдельного гражданина. Сегодня информация поднялась на такой уровень, где она стала вклиниваться в политику, стала оружием войны, сравнимым по силе с атомной бомбой. Информация уже преподала урок в виде информационной войны.

### **Информация [Information]<sup>3</sup>**

Информация (от латинского *informatio* – *разъяснение, изложение*) [4] – в самом общем понимании представляет собой меру распределения материи и энергии в пространстве и во времени, меру изменений, которыми сопровождаются все протекающие в мире процессы. В философском понимании информация приобрела смысл такой же всеобщей категории, как материя и энергия. Она рассматривается как атрибут (от латин. *attributum* - *присовокупление*), неотъемлемое свойство материи, являющееся аспектом свойства отражения.

В.А. Герасименко, указывая на чрезвычайно большую ёмкость понятия информация, его высокую неопределённость и необычность, отмечал: *«Назначение информации в самом общем виде может быть сведено к созданию условий для достижения двух целей: обеспечение устойчивости соответствующей организованной структуры (системы) и — обеспечение развития этой структуры (системы)»*[3].

Современное представление об информации включает три основных аспекта: быденный – бытийный, естественно-научный и философский. По содержанию информацию можно классифицировать по сфере применения, предназначению и др. Информация может характеризоваться также количеством, содержанием, ценностью. Количественный её аспект исследуется в основном математической статистикой, содержательный — семантической теорией. Однако само определение понятия «информация» остается предметом научных дискуссий. Существует много различных определений, каждое из которых акцентирует внимание на каком-либо аспекте информации, и поэтому не может быть принято в качестве общезначимого.

---

3 Английские эквиваленты приводятся только для тех терминов, которые представлены в терминологии по вопросам развития информационного общества (См.: Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. – М.: ИРИО. 2009.)

Академик В.М. Глушков утверждал, что *«информация существует, поскольку существуют материальные тела и созданные ими неоднородности»*. Давая свое определение информации, В.М. Глушков писал, что с одной стороны информация это совокупность возможных сведений, которые циркулируют в природе и в обществе, в том числе и в созданных человеком технических системах. С другой стороны он рассматривал информацию как *«меру неоднородности в распределении энергии или вещества в пространстве и во времени»*[5].

Н. Винер предположил, что *«информация должна переноситься каким-то физическим процессом, например, какой-то формой излучения на очень низком энергетическом уровне»*[6]. Материальными носителями информации являются знаки и сигналы, в качестве которых используются состояния физических объектов или полей, а соответствие между сигналом и содержащейся в нем информацией устанавливается по определенным правилам (кодам).

Ряд авторов, например, А.Д. Урсул рассматривает информацию, как форму существования материи, подобно массе и энергии [7]. По мнению Блюменау информация *«действительно не вещество и не энергия, а продукт научного познания, средство излучения реальной действительности в рамках, допустимых методологией информационного подхода»*[8]. В философском аспекте информация выступает и как свойство, и как форма материи.

Интуитивно понятное определение информации дал автор «Словаря русского языка» С.И. Ожегов: *«Информация — это, во-первых, сведения об окружающем мире и протекающих в нем процессах; и, во-вторых, сообщения, осведомляющие о положении дел, о состоянии чего-либо»*[9]. В обыденном понимании и правовой сегодня трактовке информация — это сведения (сообщения, данные) независимо от формы их представления.

Научно-технический прогресс вызвал необходимость расширения понятия информации в его естественно-научном смысле. При этом оно включило обмен сведениями не только между людьми, но и техническими системами (автоматами), обмен сигналами в животном и растительном мире, а также получило количественную интерпретацию. В естественно-научном понимании информация — это результат (следы) взаимодействия объектов и явлений (процессов) материального мира. Чем отчетливее следы и сильнее выражено соответствие, тем полнее состояния одного объекта отражают состояния другого объекта, тем больше информации один объект содержит о другом.[10]

По настоящее время имеет место дискуссия, является ли информация свойством всего материального, или – только живых организмов, или – исключительно разумных, сознательно действующих существ. А.А. Стрельцов, например, полагает, что информация представляет собой результат отражения движения объектов материального мира в системах живой природы, а *«описание закономерностей развития систем неживой природы не требует использования этого понятия»*. Им обосновано и предложено такое определение: *«Информация есть запечатлённый в организме результат отражения движения объектов материального мира, используемый для адаптации к изменениям окружающей действительности»*[11].

Теория связи К. Шеннона, опирающаяся на количественную меру информации, явилась первым шагом в становлении теории информации. Однако жизнь

показывает, что становление науки об информации должно быть продолжено в направлении учёта качественных характеристик информации.

Специалист в области телевидения, российский учёный В.А. Хромов предложил ввести индекс информации, определив его как отношение количества полезной информации к суммарному количеству полезной и ложной информации. Прогресс познания должен оцениваться не только скоростью роста суммарной информации, но и изменением индекса информации. Из принципа неопределенности следует, что индекс создаваемой информации всегда меньше единицы. В условиях ограниченности времени и пропускной способности канала передачи полезная информация «тонет» в ложной информации, если её индекс меньше некоторого порогового значения. Для достойной жизни человеку нужна полезная, а не ложная информация, виртуализация же, например, ведёт к росту количества ложной информации.[12]

Информацию, которая обеспечивает выполнение обществом функций социальной системы, относят к социальной информации, регулирование её оборота включается в правовую сферу. С позиции правовых норм информация по её доступности подразделяется на открытую (общедоступную) и ограниченного доступа. Массовая информация представляет собой сведения, предназначенные для неограниченного круга лиц.

Социальная информация всегда имеет цель, а целевая информация — понятие, имеющее качество. Наиболее важными в практическом плане качественными характеристиками информации являются ценность, достоверность и своевременность. С точки зрения потребителя, например, качество используемой при управлении производством информации позволит получить дополнительный экономический или социально-моральный эффект.[13]

Широко распространённым, легальным и общепризнанным социальным явлением является тайна и засекречивание информации. С позиций владельца (обладателя) информации — сохранение в тайне, например, коммерчески важной информации позволит ему успешно конкурировать на рынке производства и сбыта товаров и услуг. Вследствие этого предусматриваются законодательные гарантии защиты конфиденциальной информации.

Возрастание роли и значения компьютерной информации вызвало необходимость правового регулирования сферы её использования как специального объекта правовой защиты. Повсеместное распространение информационных технологий повлекло за собой увеличивающийся массив специальных нормативных актов об информатизации, информационных технических средствах, информационных сетях, информационной безопасности и др. с соответствующей этим отраслям знаний терминологией.

В настоящее время практически во всех отраслях законодательства и права имеется достаточно большое количество нормативно-правовых актов, правовых институтов и норм информационного характера и содержания. В большинство этих законов и во многие подзаконные нормативно-правовые акты включены дефинитивные нормы о понятиях, терминах и об определениях, которые фактически несут понятийно-категориальную информацию о явлениях и процессах (событиях, фактах и др.) Однако зачастую оказывается, что это процессы технического характера с соответствующей им «неюримдизированной» информационной терминологией.[14]

С учётом сказанного, авторы с прагматических позиций предлагают использовать такое определение понятия информация: *«Информация — это результаты (следы) взаимодействия объектов (предметов, средств) и явлений (процессов) материального мира, воспринимаемые социальным объектом (человеком) или техническим устройством (автоматом) в виде сведений (сообщений, данных) в различной форме их представления и служащие ему источником получения, передачи и накопления знаний (принятия решений, адаптации к изменениям окружающей среды)».*

## **Коммуникация [Communication]**

Коммуникации (от лат. *communico* — *делаю общим, связываю, общаюсь*) [4]. В современном понимании это: во-первых, средства сообщения (транспортные коммуникации) и связи; во-вторых, процесс обмена информацией (связь, передача сообщений, информационные контакты); в-третьих, смысловой аспект социального взаимодействия. Английское слово communication(s) означает как связь, так и общение, показательно, однако, что в англоязычных Wiki ресурсах эти понятия зачастую объединяются.[15]

Известны три типа взаимодействия в человеческом обществе: а) материальный, б) энергетический, в) информационный. Информационный обмен заключается в процессе передачи информации между социальным субъектом, называемым коммуникатором, и социальным объектом – коммуникантом (или группами этих социальных объектов). Основой информационного обмена в социальных системах является информационная деятельность — деятельность субъектов коммуникации по производству, использованию и передаче информации.

Социальный субъект понимается как активно действующий, обладающий сознанием и волей индивид или социальная группа, а социальным объектом может быть как отдельный человек, так и группа людей. Люди не связываются между собой непосредственно, образуют связи через общие объекты. При этом социальные сервисы позволяют людям создавать социальные объекты и добавлять к этим объектам собственные ценности.

В процессе информационной деятельности возникают информационные отношения — общественные отношения, складывающиеся в процессе сбора, обработки, хранения, передачи, получения и распространения информации. Информационные отношения регулируются нормами информационного права.

Для практического осуществления коммуникации используется наличествующий канал связи — физическая среда передачи информации. Такой канал включает в себя средства или пути, с помощью которых и по которым в коммуникативном процессе (процессе общения) передается информация между коммуникатором и реципиентом (аудиторией). Если информация передается с использованием технических средств, то речь идет о такой разновидности канала связи, как канал передачи данных — физическая среда, по которой передается информация из одного технического устройства в другое.

Коммуникация между людьми имеет ряд специфических особенностей, в частности, существуют возможности взаимного влияния партнеров друг на друга и вероятность возникновения коммуникативных барьеров (в этом слу-

чае четко выступает связь, существующая между общением и отношением). Каналы средств массовой информации и массовой коммуникации являются сегодня одновременно средством интерактивной коммуникации между властью, политической и экономической элитой и остальным обществом, а также односторонним инструментом информационно-психологического воздействия их владельцев на потребителей информации. Зачастую это воздействие осуществляется помимо воли адресата, например, когда информирование выступает в роли некоего фона в местах, где человек в то или иное время вынужден находиться. Что бы по этим каналам не распространялось, человек не может повлиять на источник информационно-психологического воздействия и, таким образом, вынужден воспринимать информацию, в которую могут быть вплетены психологические манипуляции.[16]

В организационно-правовом аспекте информационный обмен в социальной системе представляет собой передачу информации ее обладателем пользователю. Для того, чтобы избежать возможных негативных последствий от деструктивных действий в процессе информационного обмена, осуществляется правовое регулирование информационных процессов в обществе.[17]

## **Воздействие**

Это внешнее действие на элемент (совокупность элементов) системы или одного элемента системы на другой, в результате которого изменяются процессы, протекающие в этой системе. Воздействие может быть непосредственное (контактное) и опосредованное (дистанционное, с помощью чего-либо).

Воздействие может быть *возмущающим* или *управляющим*. Воздействие возмущающее — стремится нарушить функциональную связь между задающим на входе системы возмущением и регулируемой выходной величиной. Воздействие управляющие — обеспечивает исполнение требований в части желаемых или предсказуемых реакций системы на возмущение [18]. При этом важно отметить, что признаком устойчивости системы к воздействию является критерий «хорошей организации по Зоммергофу», предполагающий, что изменившиеся условия (множество возмущений и опасностей), в том числе и внешняя среда, не должны явиться причиной изменения равновесного состояния системы.[19]

Признание зависимости (взаимообусловленности) между входным возмущением и выходными реакциями системы позволили Норберту Винеру применить бихевиористический (от англ. *behavior* — *поведение*) [4] метод для исследования информационных систем, дав им классификацию по признаку активного (целенаправленного или нецеленаправленного – случайного) и пассивного поведения.[6] По мнению авторов, подобный подход сегодня лежит в основе понятия «управляющее информационное воздействие» и в теории борьбы в информационной сфере.

Информационное воздействие *как процесс управления* — это возбуждение (или торможение) в управляемой системе таких процессов, которые стимулируют желательный для управляющей стороны выбор. Этот вид воздействия на противоборствующую сторону предполагает не только возможность прямого выведения из строя важнейших элементов информационной системы, но и может пред-

ставлять собой передачу ей информации, которая натолкнет лицо принимающее решение на выбор решения, при котором система снижает свою эффективность. При этом надо учитывать, что, как правило, в то же время противоборствующая сторона поступает аналогично и пытается проводить подобное управляющее информационное воздействие по отношению к воздействующей стороне.[20]

Управляющее информационное воздействие, как правило, бывает трех видов: 1) Изменение в нужную сторону исходных данных, которые использует управляемая система при принятии решений. Например, угрозы (реальные и мнимые); формирование (конструирование) исходной обстановки, в которой противоборствующая сторона принимает решения; представление тенденций развития обстановки; 2) Воздействие на сам процесс принятия решения в управляемой системе (например, воздействие на алгоритм принятия решений; снижение уровня устойчивости элементов, ответственных за принятие решений); 3) Различные сочетания первых двух видов.[21]

Наибольший интерес для информационного воздействия представляют системы критических приложений. Сегодня таковыми принято называть системы, нарушение которых приводит непосредственно к резкому ослаблению безопасности государства. Все современные системы критических приложений достаточно компьютеризированы и имеют соответствующее программное обеспечение.[13]

## **Риск [Risk]**

Риск – это характеристика ситуации, имеющей неопределенность исхода. Для большинства ситуаций, связанных с решением задач безопасности, всегда характерна неопределённость. В силу этого лицо, принимающее решение в условиях неопределённости, рискует понести определенные потери, не предотвращённый ущерб. Объекты, явления или процессы, которые при определённых условиях могут стать опасными для чего-либо в каком-то отношении, являются факторами риска.

Само слово риск (от греч. *ridsikon, ridsa — утес, скала*; от итал. *risicare — лавировать между скал, risiko — опасность*; от франц. *risdoe — опасность, буквально объезжать утес, скалу*) [4] — в общепринятом толковании это возможность угрозы или опасности потери чего – либо или неудачи. В популярном интернет-ресурсе Википедия, например, риск трактуется как сочетание вероятности и последствий наступления неблагоприятных событий. Однако в словаре С.И. Ожегова риск определяется не только как «*опасность, возможность опасности*», но и как «*действие наудачу в надежде на счастливый исход*»[9].

Сегодня предложено значительное число различных определений риска. Авторы монографии «Теория риска и моделирование рискованных ситуаций», например, приводят ряд определений понятия риск, используемых в сфере бизнеса. Так, например, риск как вероятность возникновения убытков или недополучения доходов по сравнению с прогнозируемым вариантом. Другой пример, риск как вероятность или угроза потери предприятием части своих ресурсов. Во всех таких определениях присутствует вероятностный характер данной категории, количественное измерение которой неоднозначно.[22]

Современные тенденции в управлении качеством вызвали появление руководств по менеджменту рисков. Предпринимаются попытки использовать теорию

риска и в качестве одной из базовых основ теории безопасности. В свете сказанного представляется правомерным включение категории риск в число категорий, образующих научные основы обеспечения информационной безопасности.

При этом риск может быть определен как угроза или опасность потенциально возможной (вероятностной) потери части ресурсов или как деятельность, связанная с преодолением неопределенности в ситуации выбора варианта достижения цели. В таком случае открывается возможность количественно или качественно попытаться оценить вероятность достижения предполагаемого результата или отклонения от цели, неудачу.

## **Угроза [Treat]**

К первоочередным задачам при создании теории информационной безопасности относится формирование системы базовых понятий, к которым относятся: информационная опасность, информационная угроза, информационная безопасность. Проблемы безопасности фактически порождены наличием определённых угроз и опасностей, различие же между понятиями угроза и опасность достаточно тонкие. Ряд авторов под опасностью понимают возможность (способность) нанесения ущерба, а под угрозой — намерение причинить этот ущерб.[23]

Словарь русского языка толкует понятие угроза двояко: первое значение — *«запугивание, обещание причинить вред»*; второе значение — *«возможная опасность»*[24]. В широком смысле угроза — это потенциальная возможность нарушения защиты чего-либо или кого-либо.

Угрозы объектам безопасности могут быть реальными и потенциальными, могут исходить от внутренних и внешних источников. Следствием информационных угроз может являться возникновение совокупности факторов и условий, создающих опасность нанесения вреда жизненно важным интересам человека, общества и государства в информационной сфере.

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащённости и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Словарь терминов МЧС (2010) включает понятие: *«Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реальную опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее»*. Популярными словарями по информационной безопасности трактуют угрозу как совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности, потенциальная возможность нарушения защиты.[25-28]

В нормативных документах Республики Беларусь, например, применительно к сфере информационных технологий стандартизовано понятие: *«Угроза — потенциально возможное событие, приводящее к нарушению свойств (конфиденциальности, целостности, доступности) информации при её хранении, преобразовании и передаче»*[29].

## Опасность

Опасность — это одно из основных понятий теории национальной безопасности наряду с вызовом, риском и угрозой, занимающее в их иерархии место между риском и угрозой. По размаху и масштабам возможных негативных последствий опасности могут быть глобальные, региональные, национальные, локальные, частные.

Словарь терминов МЧС (2010), например, трактует опасность как возможность возникновения обстоятельств, при которых материя, поле, энергия, информация или их сочетание могут таким образом повлиять на сложную систему, что приведет к ухудшению или невозможности ее функционирования и развития. Стандарт по пожарной безопасности технологических процессов (ГОСТ Р.12.03 47-98), например, оперирует понятием: «*Опасность — потенциальная возможность возникновения процессов или явлений, способных вызвать поражение людей, нанести материальный ущерб и разрушительно воздействовать на окружающую атмосферу*».

Опасность — свойство, внутренне присущее любой сложной системе. Она может реализоваться в виде прямого или косвенного ущерба для объекта (предмета) воздействия постепенно или внезапно, и резко в результате отказа системы. Определяющие признаки опасности — возможность непосредственного деструктивного воздействия на объект (предмет, средство) воздействия; возможность нарушения его нормального состояния функционирования или протекания процесса. Наличие хотя бы одного из определяющих признаков является достаточным для отнесения факторов к разделу опасных (вредных). Количество признаков, характеризующих опасность, определяется в зависимости от целей анализа.[30]

## Безопасность [Safety (Security)]

В словаре современного русского языка понятие «безопасность» трактуется как отсутствие опасности, состояние, при котором кому-либо, чему-либо не угрожает опасность, а также в значении защищенный, огражденный от опасности, не грозящий опасностью для кого-нибудь, кому-нибудь; безвредный.[24]

В зарубежной литературе, в английском словаре «Webster's new twentieth century dictionary of the English language. Second edition» (1979), например, безопасность рассматривается как нечто общее, присущее способам предотвращения ущерба, вызываемого воздействием опасных факторов, например, несчастных случаев, представляющее собой свойство не субъекта или объекта, а метода взаимодействия субъекта и объекта: так, безопасность – это качество или условие оставаться неврежденным.

Нередко на практике значение понятия «безопасность» зависит от контекста, в котором оно используется, что свидетельствует о многообразном толковании данного понятия. В контексте технической терминологии, как правило, отражается только какая-либо одна сторона исследуемого понятия, например: «безопасность – свойство объекта не допускать ситуаций, опасных для людей и окружающей среды» (например, [31]); или «безопасность – способность системы функционировать,

не переходя в опасные состояния, угрожающие здоровью и жизни людей или наносящие другой ущерб в больших масштабах» (например, [32]).

Ряд исследователей, рассматривающих различные аспекты жизнедеятельности человека, говоря о психофизиологических факторах системы «человек – машина», определяет безопасность как способность противостоять воздействию внутренних и внешних возмущений, действующих на отдельные элементы этой системы и на связи между ними.[21] В популярном словаре терминов по информационной безопасности, например, приведено такое определение: «Безопасность — свойство системы противостоять внешним и внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные её состояния или поведение»[25].

Анализируя приведенные выше определения можно придти к выводу о том, что понятие «безопасность» является комплексным. На взгляд авторов определение этого понятия должно содержать наиболее существенные признаки, наиболее полно раскрывающих определяемое понятие. К таким признакам относятся:

1. Сущность трактуемого понятия: безопасность — это защищенность от угрозы опасности.
2. Объект, состояние которого характеризуется рассматриваемым определением, например, человек, общество и государство.
3. Характеристики (параметры, свойства) объекта, на который распространяется данное определение, например, жизненно важные интересы человека, общества и государства.
4. Специфический для рассматриваемого объекта вид противостоящего ему воздействия, например, информационные угрозы.

С учетом изложенного, под безопасностью в прагматическом аспекте, по мнению авторов, можно понимать такое состояние (положение) объекта (предмета, средства, процесса), при котором его характеристики (свойства, способности) и условия деятельности (протекания, проявления) сводят к минимуму эффективность деструктивного воздействия за счет наличия и успешного использования системы мероприятий, обеспечивающих защищенность от известных средств и методов подобного воздействия.

## **Система [System]**

Система (от греч. *systema* — *целое, составленное, соединенное из частей*) [4] — термин, используемый в тех случаях, когда хотят охарактеризовать исследуемый объект как нечто целое (единое), сложное, о котором невозможно сразу дать представление, показав его, изобразив графически или описав математическим выражением.

Существует несколько десятков определений этого понятия. Их анализ показывает, что определение понятия система изменялось не только по форме, но и по содержанию. В одних определениях в той или иной форме говорится о том, что система — это элементы (части, компоненты) и связи (отношения) между ними. Так, Л. фон Берталанфи определял систему как «*комплекс взаимодействующих компонентов*» или как «*совокупность элементов, находящихся в*

*определенных отношениях друг с другом и со средой»*[33].

Далее, в определениях системы появляется понятие цель. Сначала — в неявном виде в определении Ф.Е. Темникова: «*система — организованное множество*», в котором цель появляется при раскрытии понятия «организованное». Затем — в работах В.И. Вернадского, У.Р. Гибсона, П.К. Анохина и М.Г. Гаазе-Рапопорта в виде конечного результата, системообразующего критерия, функции, а позднее и с явным упоминанием о цели.

Затем в определение системы наряду с элементами, связями и целями начинают включать наблюдателя, т.е. лицо, представляющее объект или процесс в виде системы при их исследовании или принятии решения. На необходимость учета взаимодействия между изучаемой системой и исследователем указывал ещё У.Р. Эшби [19]. Но первое определение, в котором в явном виде включен наблюдатель, дал Ю.И. Черняк: «*Система есть отражение в сознании субъекта (исследователя, наблюдателя) свойств объектов и их отношений в решении задачи исследования, познания*»[1].

В период становления системных исследований в 60-70 годах прошлого века довольно часто возникали дискуссии о том, материальны или нематериальны системы. Стремясь подчеркнуть материальность систем, некоторые исследователи в своих определениях заменяли термин элемент терминами вещь, объект, предмет. Хотя последние можно трактовать и как абстрактные объекты или предметы исследования, все же авторы этих определений явно хотели обратить внимание на овеществленность, материальность системы.

Бессмысленность спора о материальности и нематериальности системы показал В.Г. Афанасьев в следующей цепочке рассуждений: «*От объективно существующей системы — к понятию системы; от понятия системы, используемого как инструмент познания системы, снова к реальной системе, знания о которой обогатились нашими системными представлениями — такова диалектика объективного и субъективного в системе*»[1]. Таким образом, в понятии система объективное и субъективное составляют диалектическое единство, и следует говорить не о материальности или нематериальности системы, а о подходе к объектам исследования как к системам, о различном представлении их на разных стадиях познания или создания.

Системы могут быть естественными и целевыми (специально созданными человеком). Целевые системы, как правило, являются организационно – техническими, с явной функцией управления. При этом любая система характеризуется составом и структурой. Состав — это совокупность предметов (элементов, признаков), образующих целое. Структура — внутреннее устройство, совокупность устойчивых связей целого, обеспечивающих его целостность и сохранение основных свойств при различных воздействиях.

В современном представлении наиболее часто используется определение системы как нечто целого, представляющего собой единство закономерно расположенных и находящихся во взаимной связи частей (элементов, предметов, явлений), объединение которых придает системе свойства, не присущее каждой из частей в отдельности.

С учетом вышеизложенного и опираясь на философский анализ сущности понятия «система» авторы полагают, как и в случае с категорией «информация»,

целесообразным отнесение понятия «система» к категории теории отражения. Понятие «система», как и понятие «информация», может быть представлено в различных аспектах: от философского (теоретико-познавательного) или научно-исследовательского до материального.

## **II. ТЕРМИНЫ, ОПРЕДЕЛЯЮЩИЕ ПРЕДМЕТНУЮ ОСНОВУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Большой энциклопедический словарь определяет понятие предметная область как часть реального мира, рассматриваемую в пределах данного контекста. Под контекстом понимается область исследования или объект некоторой деятельности. В связи с этим авторы отнесли ко второй группе обсуждаемых термины, обозначающие понятия и их структурные связи с другими понятиями в области информационной безопасности как в специфической области знаний. Логично предположить, что эта область постоянно наполняется новыми понятиями, дополняющими систему знаний и данный процесс бесконечен.

### **Информационная система [Information system]**

Одно из системообразующих понятий информационной безопасности — информационная система. Легальное определение понятия информационной системы было приведено в российском законе «Об информации, информатизации и защите информации» как организационно упорядоченной совокупности документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.[14]

В проекте Конвенции об обеспечении международной информационной безопасности термин «информационная система» определяется как совокупность содержащейся в базах данных информации и обеспечивающих её обработку технических средств.[34]

С прагматических позиций авторы предлагают использовать такое определение: *«Информационная система — это естественная (биологическая) или целевая (организационно-техническая) совокупность объектов, закономерно расположенных и находящихся во взаимной связи, совокупность сведений об объекте (предмете, средстве, явлении, процессе), о его деятельности (проявлении, протекании), а также используемые информационные технологии».*

### **Информационный поток**

Несмотря на наличие ряда монографий, посвященных теории информационных потоков, следует отметить, что достаточно полное определения этого термина в настоящее время в литературе отсутствует.

Специалисты в области программирования называют потоком абстрактное понятие, относящееся к любому переносу данных от источника к потребителю. В обыденной практике чаще всего используются упрощенные и достаточно проти-

воречивые определения, например: информационные потоки — это пути передачи информации, обеспечивающие существование социальной системы, внутри которой они двигаются. Это процессы передачи информации для обеспечения взаимосвязи всех звеньев социальной системы.

Наиболее полное, по мнению авторов, определение понятия информационного потока приводится в теории логистики — учении о планировании, управлении и контроле движения материальных, информационных и финансовых ресурсов в различных системах.[35]

С учетом приведенных рассуждений, авторы статьи предлагают следующее рабочее определение: *«Информационный поток — это генерируемая совокупность сведений (сообщений, данных) независимо от формы их представления, циркулирующих в системе, а также между системой и внешней средой, предназначенных для реализации сигнальных и управляющих функций».*

### **Информационные процессы [Information process]**

Процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации — информационные процессы — это деятельность субъекта и функционирование естественных и технических средств в информационной сфере. Под деятельностью при этом авторы понимают генерирование (производство), добывание, хранение, переработку, передачу, использование и защиту информации.[3,13]

Прежде чем пытаться подойти к определению важнейшего понятия информационная сфера, на взгляд авторов необходимо определиться с такими понятиями как информационный объект, информационный ресурс и информационная инфраструктура.

### **Информационный объект [Information object]**

К информационным объектам относятся объекты материального мира, реализующие функции генерации (производства, воспроизводства), сбора и накопления, хранения, переработки и передачи информации.[3,13]

### **Информационный ресурс**

Информационные ресурсы — это информационная инфраструктура и её потоки. Понятие информационный ресурс включает в себя как сведения сами по себе, так и сведения в базах данных информационных систем. База данных — объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Помимо научной литературы, понятие информационные ресурсы вошло в нормативные правовые акты. Свою легализацию это понятие получило в российском законе «Об информации, информатизации и защите информации» (1995 год, в настоящее время утратил силу) как отдельные документы и отдельные массивы документов, документы и массивы документов в информаци-

онных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).[14]

## **Информационная инфраструктура**

Информационная инфраструктура представляет собой совокупность систем, средств и технологий генерации, добывания, переработки и передачи информации, а также систем и средств, обеспечивающих защищенность информационных систем и информационного ресурса от угроз деструктивного воздействия. Один из первых популярных русскоязычных словарей-справочников по информационной безопасности приводил такое определение понятия: «Информационная инфраструктура – совокупность центров обработки и анализа информации, каналов информационного обмена и телекоммуникации, линий связи, систем и средств защиты информации»[25].

По мнению авторов, сложная организация взаимодействия информационной инфраструктуры и пользователей (потребителей: человека, отдельных групп людей и общества в целом) может быть условно представлена в виде иерархии отдельных уровней (страт):

Страта 1. *Пользовательский слой* — слой генераторов и потребителей информационного ресурса с правилами их взаимодействия с информационной структурой.

Страта 2. *Функциональный слой* с совокупностью услуг, предоставляемых пользователям (потребителям) различными поставщиками информации.

Страта 3. *Информационный слой*, в котором непосредственно содержится информационный ресурс.

Страта 4. *Коммуникационный слой*, рассматриваемый как единая информационная магистраль (информационная сеть).

Такое представление позволит «не потерять» в описываемом взаимодействии человека, как центра информационной инфраструктуры, ради удовлетворения информационных потребностей которого она и организуется.

Заметим также, что Модельный информационный кодекс, принятый МПА СНГ, ввел правовое понятие «информационно-инфраструктурные отношения», определив их как «*общественные отношения, возникающие в процессе создания, распространения, использования, хранения и уничтожения (утилизации) информации, а также в процессе деятельности субъектов информационной инфраструктуры, предоставления информационных услуг и выполнения работ в информационной сфере, использования информационных технологий и ресурсов и обеспечения информационной безопасности*»[36].

## **Информационная сфера [Information sphere]**

Авторы полагают, что понятие информационная сфера следует определять в двух аспектах: как пространство и как деятельность.

Информационная сфера (*как пространство*) представляет собой совокуп-

ность информационного ресурса, информационной инфраструктуры, а также информационных объектов и субъектов, использующих информацию.

Информационная сфера (*как деятельность*) связана с функционированием естественных и технических объектов (средств, предметов) генерации, пространства, обработки и потребления информации.[14]

В документах ООН получило своё отражение понятие «информационное пространство», трактуемое как *«сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая общественное сознание, информационно-телекоммуникационную инфраструктуру и собственную информацию»*[34].

## **Информационный риск**

По аналогии с определением общего понятия риск под информационным риском следует понимать угрозу информационной безопасности или информационную опасность потенциально возможной (вероятностной) потери части (или качества) информационного ресурса или деятельность, связанную с преодолением неопределенности в обеспечении информационной безопасности. В таком случае представится возможным попытаться количественно или качественно оценить вероятность достижения предполагаемого результата или отклонения от заданной цели, т.е. неудачу.

В настоящее время уже появились соответствующие стандарты для области информационных технологий (например, британский стандарт BS 7799-3/2006 – «Руководство по менеджменту рисков информационной безопасности»). Вышел в свет международный стандарт ИСО/МЭК 27005: 2008 «Информационные технологии. Средства обеспечения безопасности. Риск-менеджмент информационной безопасности» и ряд других.

## **Угрозы информационной безопасности (информационные опасности)**

Как отмечалось выше, угроза информационной безопасности — это информационная опасность, реализация которой становится весьма вероятной, фактор или совокупность факторов, создающих опасность функционированию и развитию информационной среды общества. Такими факторами могут быть действия, поведение объектов, природные явления и т.д. Следует отметить, что в настоящее время не сложилось системного представления классификации угроз информационной безопасности. В основу классификации угроз безопасности информации закладывается содержание факторов, на неё воздействующих.[23]

## **Информационное оружие [Information weapon]**

Для воздействия на информационную сферу применяют различные виды информационного оружия. Современные реалии таковы, что не только в научной, но и в общественно-политической лексике достаточно часто можно встретить такое понятие как «информационная война» [*Information war*] — противобор-

ство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, а также массивной психологической обработки населения с целью дестабилизации общества и государства.

Информационное оружие представляет собой совокупность средств, методов и технологий, обеспечивающих возможность силового воздействия на информационную сферу противника с целью разрушения его информационно-инфраструктуры, систем управления государством, снижения обороноспособности. К информационному оружию могут быть отнесены и специальные устройства и средства, конструктивно предназначенные для воздействия на информационный ресурс, информационную среду, носителей информации, информационные процессы, а также на субъекты, использующие информацию в своей деятельности.

Информационное оружие подразделяется на два основных вида: информационно-техническое и информационно-психологическое оружие. Различают стратегическое, оперативное и тактическое информационное оружие. Информационное оружие позволяет целенаправленно активизировать в информационной сфере противостоящей стороны такие процессы, в которых заинтересован субъект, применяющий подобное оружие. Как правило, эти процессы направлены на самоуничтожение или нарушение функционирования социальной или соответствующей информационно-технической системы противостоящей стороны.[20]

В отличие от тех исследователей, которые относят к информационному оружию только «методы и способы воздействия», авторы не без основания считают, что информационное оружие представляет собой материальные устройства и средства и воздействует на объекты и субъекты материального мира. При этом не исключается и опосредствованное воздействие на информацию, как на следы взаимодействия объектов материального мира.

## **Информационная безопасность [Information security]**

Попытаемся проанализировать, какое контекстное значение понятия «информационная безопасность» будет наиболее точно и полно соответствовать вкладываемому в него смыслу.

1. Безопасность как свойство или *способность системы* не допускать опасных состояний, не переходить в них.

Как любая система с обратной связью, информационная система обладает способностью к самосохранению, однако ограничить поддержание безопасности исключительно реакцией самой системы на деструктивные воздействия (информационные угрозы или опасности) будет неправомерно. Цели и алгоритмы управления формируются за пределами собственно информационной системы, а они также обуславливают способность данной системы не переходить в опасные состояния.

2. Безопасность как *состояние системы*, исключающее возможность опасного события и как такое условие протекания процесса, в котором исключается

деструктивное воздействие на систему.

В подобной трактовке информационная безопасность представляет собой временную характеристику функционирования информационной системы. Вполне оправдано, может быть, применение такой характеристики к конкретному элементу или к группе элементов системы в рамках заданного интервала времени или определенных условий.

3. Безопасность как *система мероприятий*, обеспечивающих защиту системы от деструктивных воздействий (система обеспечения информационной безопасности).

Данная трактовка понятия подразумевает активное противостояние опасным для возможного использования информационного ресурса факторам. Она охватывает организационно-технические, правовые и социальные меры, обеспечивающие защиту информационной системы от деструктивного воздействия.

С учётом изложенного, система обеспечения информационной безопасности должна быть нацелена на обеспечение информационной безопасности как свойства и как состояния, а также на создание безопасных условий для использования информационного ресурса как вида деятельности.[11,13,17]

В формате ОДКБ существует согласие относительно того, что под информационной безопасностью понимается состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве. Такая трактовка понятия «информационная безопасность» полностью совпадает с его определением, содержащемся в тексте соглашения о международной информационной безопасности государств Шанхайской организации сотрудничества.[34]

### **Объект обеспечения информационной безопасности**

Объекты обеспечения информационной безопасности — это объекты материального мира, реализующие в себе функции генерации, добывания, переработки, передачи информации и обладающие программами реализации этих функций. К таким объектам относятся как собственно информация, например, сообщение, знание, мировоззренческая картина и др., так и носитель информации. Носитель информации может быть неодушевленным — техническим, одушевленным — социальным или, как правило, социально-техническим.[13,21]

Основными объектами правового обеспечения безопасности в информационной сфере являются общественные отношения и внешние и внутренние угрозы, могущие нанести ущерб предметам и интересам субъектов этих отношений.

### **Информационный потенциал**

Известно, что в процессе борьбы в информационной сфере любые информационные воздействия как наступательного, так и оборонительного характера в конечном итоге влияют (в положительную или в отрицательную сторону) на информационные потенциалы противоборствующих сторон. При этом под *информационным потенциалом* (от лат. *potentia* – *возможность, мощь*), по

мнению авторов, следует понимать возможность (способность) своевременно генерировать, добывать, перерабатывать и передавать определённые (необходимые) объёмы информации соответствующего качества.

Информационный потенциал зависит от количественных и качественных характеристик информационного ресурса и информационных технологий. Именно соотношение информационных потенциалов противоборствующих сторон, в конечном счете, определяет превосходство в борьбе в информационной сфере.[21]

### **Информационное превосходство**

Информационное превосходство — это способность более эффективно добывать, перерабатывать и распределять непрерывный поток информации о складывающейся в реальном масштабе времени обстановке, препятствуя противоборствующей стороне делать то же самое.

В научной литературе и публицистике всё чаще встречается: в разных контекстах «цифровой» или «информационный суверенитет». Представляется, что эти понятия следует различать. Информационный суверенитет (суверенитет государства в национальном информационном пространстве) можно трактовать как право государства определять свою информационную политику самостоятельно, распоряжаться инфраструктурой, ресурсами, обеспечивать информационную безопасность. Например, проект закона Украины «О национальной программе информатизации» предлагал такое определение: *«Информационный суверенитет государства – способность государства контролировать и регулировать потоки информации из-за пределов государства с целью <...> гарантирования национальной безопасности».*

## **III. ТЕРМИНЫ, ОПРЕДЕЛЯЮЩИЕ ОСНОВЫ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

К третьей группе терминов авторы отнесли термины, характерные для деятельности в области обеспечения информационной безопасности. Такая деятельность может быть многоплановой. Термины этой группы обозначают широкий круг понятий различного уровня: от сигнального до системного.

### **Обеспечение информационной безопасности**

На государственном уровне обеспечение безопасности понимается как проведение единой государственной политики в области безопасности. Обеспечение информационной безопасности государства — это процесс, содержание которого составляет проведение единой государственной политики в виде системы мер организационно-технического, правового, социального и иного характера, адекватных угрозам жизненно важным интересам человека, общества и государства в информационной сфере.[25-29]

Приводимые в справочной литературе определения обеспечения информа-

ционной безопасности чаще преломляются либо к национальной безопасности (в рамках доктринальных трактовок), либо к отдельным объектам обеспечения безопасности. Так, например, пособие Министерства обороны Республики Беларусь в области защиты информации приводит понятие: «*Обеспечение информационной безопасности в сети электросвязи — деятельность, направленная на поддержание информационной безопасности сети электросвязи*»[29].

### **Система обеспечения информационной безопасности**

Система обеспечения информационной безопасности — это целенаправленная совокупность взаимосвязанных организационно-технических, правовых и социальных норм и механизмов, направленных на противодействие угрозам информационной безопасности с целью сведения до минимума возможного ущерба в информационной сфере.[25]

Справочное пособие Министерства обороны Республики Беларусь в области защиты информации приводит понятие: «*Обеспечение информационной безопасности в сети электросвязи — совокупность правовых норм, организационных и технических мероприятий, служб информационной безопасности сети электросвязи и средств безопасности сети электросвязи, органов управления и исполнителей, направленных на обеспечение информационной безопасности сети электросвязи*»[29].

### **Информационная защищенность**

В публикациях используется термин «информационная защита» как совокупность средств, обеспечивающих противодействие внешнему информационному воздействию (включая информационные атаки), а также информационных средств, предназначенных для противодействия реализуемым по каналам распространения информации (СМИ, сети передачи данных и т.п.) психологическим воздействиям.[37] Словарь терминов МЧС (2010), например, трактует это понятие как организационные, правовые, технические и технологические меры по предупреждению угроз информационной безопасности и устранению их последствий.

В соответствии с предложенным системным подходом под информационной защищенностью авторы понимают состояние элемента информационной системы, при котором обеспечены необходимые и достаточные условия его надежного, устойчивого и эффективного функционирования.

### **Безопасность информации**

Безопасность информации — это состояние защищенности информации, в том числе обрабатываемой средствами вычислительной техники, от угроз деструктивного воздействия. Это состояние, при котором с требуемой степенью обеспечивается защищенность информации от утечки, хищения, утраты, несанкционированного уничтожения, разрушения, искажения, модификации, копирова-

ния и блокирования.[25-28]

Так, например, в нормативных правовых и технических нормативных правовых актах Республики Беларусь в области защиты информации понятие безопасности информации трактуется как состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и. т.п.[29]

## **Защита информации [Information protection]**

Информация является одним из наиболее ценных ресурсов, поэтому обеспечение защиты информации является одной из важнейших и приоритетных задач. Под защитой информации понимается процесс обеспечения сохранности, целостности и надежности сведений (данных).

Защита информации представляет собой принятие комплекса организационно-технических, правовых и социальных мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации.

Защита информации с необходимостью также должна предусматривать совокупность организационных, правовых, технических и технологических мер по предотвращению и отражению угроз информационным ресурсам и информационным системам, по устранению последствий таких угроз.[25-29]

## **Система защиты информации**

Для защиты информации создается система защиты информации, состоящая из совокупности органов и (или) исполнителей, используемой ими техники защиты, организованная и функционирующая по правилам, установленным правовыми, распорядительными и нормативными документами в области защиты информации.

Система защиты информации — это целенаправленная совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов и механизмов защиты.[25-29]

## **Объект защиты информации**

Объектами защиты информации являются информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечить защиту в соответствии с поставленной целью защиты информации.[25-29]

## **Администратор защиты [Security administrator]**

Администратор защиты — субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.[25-29]

## **Способ защиты информации**

Известно, что способ — это избранное действие или система действий (комплекс определенных мер, мероприятий, приемов), применяемых при выполнении какой-либо работы или осуществлении чего-либо, а также закономерный порядок и последовательность (упорядоченная последовательность) их применения.

Способ защиты информации — это порядок и правила применения определенных принципов и средств защиты информации, обоснованная совокупность мероприятий и действий, составляющих сущность защиты информации, а также определенный порядок применения средств защиты информации при решении конкретных задач.[25-29]

## **Средства защиты информации**

Средства защиты информации — технические, криптографические, программные и другие средства, а также системы управления комплексами средств, предназначенные и используемые для защиты и контроля эффективности защиты информации.[22-29]

## **Носитель информации**

Носителем информации может быть любой материальный объект, в том числе физическое поле, в котором информация отображается в виде символов, образов, явлений или, например, технических решений и процессов. С появлением электронно-вычислительных машин возник такой вид информации, как компьютерная информация. Сегодня широкое распространение получили электронные носители информации.[13]

## **Обладатель информации**

Это не вполне удачный введённый в обращение юридический термин. Обладателем информации может быть физическое или юридическое лицо, общественная организация или государство, самостоятельно создавшие информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации.[25-29]

## **Доступ к информации**

Доступ к информации — это возможность получения информации, в том числе и с целью её дальнейшего использования. Доступ представляет собой специальный тип взаимодействия между субъектом и объектом информационного обмена, в результате которого создается поток информации от одного к другому.

Доступ у информации предполагает получение субъектом возможности ознакомления с информацией, включая возможности её обработки, в частности, копирования, модификации или уничтожения, в том числе при помощи технических средств. Предоставление субъекту некоторых прав доступа к информационному обмену называется авторизацией.

В сфере защиты государственных секретов понятие «доступ к секретной информации» трактуется как санкционированный процесс ознакомления с секретной информацией физического лица, имеющего допуск к такой секретной информации.[25-29,38]

## **Объект доступа**

Объект доступа — единица информационного ресурса, доступ к которому регламентируется правилами разграничения доступа.[27]

## **Несанкционированный доступ к информации**

Несанкционированный доступ к информации — это процесс, нарушающий принятые или установленные обладателем информации правила разграничения доступа к ней, следствием которого могут быть утечка, искажение, разрушение, уничтожению, блокированию информации, а также утрата, уничтожение или сбой функционирования носителя информации.[26-30,38]

## **Воздействие на информацию**

Под воздействием на информацию понимается система мероприятий, оказывающих влияние на количественное или качественное (смысловое) содержание информации, циркулирующей в информационных системах, проводимых с целью преднамеренного искажения, задержки распространения, разрушения или уничтожения в процессе ее генерации, переработки или передачи.

В словарной литературе встречаются также понятия: «Воздействие на информационное пространство (силовое)» — нарушение с использованием информационного оружия нормального (установленного законными собственниками, владельцами и пользователями) функционирования информационной инфраструктуры общества, правил формирования, хранения и распространения информации и информационных ресурсов и «Воздействие информационно-психологическое» — применение информационно-психологических способов и средств воздействия на психику человека с целью её модификации в нужном для воздействующей стороны направлении» [16,20,21].

## Литература

1. Системный анализ и принятие решений. Словарь - справочник под общей редакцией Волковой В.Н. – М.: «Высшая школа», 2004.
2. Блауберг И.В., Юдин Э. Г. Становление и сущность системного подхода. – М.: «Наука», 1973.
3. Герасименко В.А. Основы информационной грамоты. – М.: Энергоатомиздат, 1996.
4. Современный словарь иностранных слов. - М.: «Русский язык», 2001.
5. Глушков В. М. О кибернетике как науке // Кибернетика, мышление, жизнь. – М.: «Мысль», 1964.
6. Винер Н. Кибернетика, или управление и связь в животном и машине. – 2-е издание. – М.: «Наука», 1983.
7. Урсул А.Д. Информация. – М.: «Наука», 1971.
8. Блюменау Д.И. Информация и информационный сервис. - Л.: «Наука», 1989.
9. Ожегов С.И. Словарь русского языка. 23-е издание, исправленное. Под редакцией члена-корреспондента АН СССР Н.Ю. Шведовой. - М.: «Русский язык», 1990.
10. Бриллиюзн Л. Наука и теория информации. – М.: «Физматгиз», 1960.
11. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовниченко и В.П. Шерстюка. – М.: МЦНМО, 2002.
12. Хромов Л.И. Теория информации и теория познания. – СПб.: Изд-во Русского Философского Общества, 2006.
13. Юсупов Р.М., Заболотский В.П. Концептуальные и научно-методологические основы информатизации. - СПб, Наука, 2009.
14. Информатика в терминах и определениях российского законодательства / Под ред. В.А. Никитова. - М.: Славянский диалог, 2000.
15. Данюшина Ю.В. Коммуникативная безопасность в государственной и деловом управлении // Язык. Словесность. Культура. 2011, №1.
16. Информационное общество: Информационные войны, Информационное управление. Информационная безопасность / Под ред. М.А. Вуса. – СПб.: ФЦП «Интеграция», Издательство СПбУ, 1999.
17. Вус М.А., Гусев В.С., Долгирев Д.В., Молдовян А.А. Информатика: Введение в информационную безопасность. – СПб.: Изд-во «Юридический центр Пресс», 2004.
18. Энциклопедия кибернетики (в двух томах). Т. 1. - Киев: Главная редакция украинской энциклопедии, 1974.
19. Эшби У.Р. Принципы самоорганизации. - М.: «Мир», 1966.
20. Расторгуев С.П. Философия информационной войны. – М.: Вузовская книга, 2001.
21. Пирумов В.С. Информационное противоборство. Четвертое измерение противостояния. – М.: «Оружие и технологии», 2010.
22. Шапкин А.С., Шапкин В.А. Теория риска и моделирование рисковых ситуаций. – М.: Издательско-торговая корпорация «Дашков и Ко», 2005.

23. Юсупов Р.М. Наука и национальная безопасность. – СПб.: Наука, 2011.
24. Словарь современного русского литературного языка: Изд. 2-е, перераб. и доп. - М.: Рус.яз. 1991.
25. Приходько А.Я. Словарь-справочник по информационной безопасности. – М.: СИНТЕГ, 2001.
26. Словарь терминов и определений в области информационной безопасности. – М.: НИЦВАГШ ВС РФ, 2008.
27. Термины и определения в области информационной безопасности / Колл. авторов. – М.: Издательство «АС-Траст», 2009.
28. Иняков А.Ф. Защита информации: термины, понятия, аббревиатуры нормативных актов и технологий. В 2-х кн.: - М.:, 2003.
29. Сборник основных терминов и определений в области защиты информации. – Мн.: НИИ ВС РБ, 2010.
30. Информационные вызовы национальной и международной безопасности / Под. общ.ред. А.В. Фёдорова, В.Н. Цигичко. – М.: ПИР-Центр, 2001.
31. Надежность технических систем: Справочник / Ю.К.Беляев, В.А. Богатырев, В.В. Болотин и др.; Под ред. И.А. Ушакова. - М.: Радио и связь, 1985.
32. Рябинин И. Надежность, живучесть и безопасность кораблей. // Мор. сборник. 1987, № 8. С. 62-65.
33. Бертуланфи Л. Общая теория систем – обзор проблем и результатов. «Системные исследования» - М.: «Наука», 1969.
34. Райзберг Б.А., Лозовский Л.Ш., Стародубцев Е.Б. Современный экономический словарь. – М.: ИНФРА-М, 2007.
35. Международная информационная безопасность: проблемы и решения / Под общ. ред. С.А. Комова. – М., 2011.
36. Модельный информационный кодекс для государств – участников СНГ // Информационный бюллетень МПА СНГ. 2013, № 57. Часть I. С.44-73.
37. Шакин Д.Н. (руководитель), Бунев Е.Г., Доценко С.М., Ильин А.П., Марголин П.С., Пирумов В.С., Тынянкин С.И. Информационная безопасность. Коллективная монография. – М.: «Оружие и технологии», 2009.
38. Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ. Сборник / Сост. Бачило И.Л., Вус М.А., Гусев В.С., Макаров О.С. – СПб.: СПИИРАН, 2011.
39. Вус М.А., Кучерявый М.М., Шакин Д.Н., Юсупов Р.М. Эскиз системного подхода к формированию понятийного аппарата информационной безопасности // Информатизация и связь – 2012, №9. С.7-15.
40. Юсупов Р.М., Шишкин В.М. Информационная безопасность и кибербезопасность: семантический конфликт и сосуществование // Информатизация и связь – 2013, №6. С.22-27.
41. Бачило И.Л., Вус М.А., Макаров О.С. К вопросу о развитии информационного законодательства СНГ // Информатизация и связь – 2014, №1. С.13-16.
42. Кучерявый М.М., Шакин Д.Н., Гвритишвили П.П. К вопросу о сущности и содержании информационной безопасности // Информатизация и связь – 2014, №1. С.17-20.

**ПОНЯТИЙНЫЙ АППАРАТ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
В НОРМАТИВНЫХ АКТАХ ГОСУДАРСТВ – ЧЛЕНОВ ОДКБ**

№	Термин	Определение понятия	Ист. <sup>1</sup>
<b>А</b>			
1	<b>Автоматизация</b>	применение <b>информационно-коммуникационных технологий</b> для обработки, систематизации, хранения и <b>передачи информации</b> с целью облегчения и вытеснения форм человеческого труда, повышения производительности и прозрачности процессов	20
		<i>В законодательстве Республики Казахстан, регулирующем информационную сферу, до 2011 г. использовалось понятие «автоматизация» (а не «информатизация»).</i>	
2	<b>Атака компьютерная</b>	целенаправленное воздействие на <b>информационные системы</b> и <b>информационно-телекоммуникационные сети</b> программно-техническими средствами, осуществляемое в целях нарушения <b>безопасности информации</b> в этих системах и сетях	30
<b>Б</b>			
3	<b>БАЗА ДАННЫХ</b>	объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ	32

<sup>1</sup> **Ист.** – Источник.

Список использованных источников приведен в конце таблицы; (е [32] — приведены авторские трактовки понятий.)

№	Термин	Определение понятия	Ист. <sup>1</sup>
		используемая в <b>информационных системах</b> совокупность данных, организованная по определенным правилам, предусматривающим общие принципы описания, хранения и оперирования данными вне зависимости от применяемых прикладных программ	11
		совокупность структурированной и взаимосвязанной <b>информации</b> , организованной по определенным правилам на <b>материальных носителях</b>	19
		интегрированная совокупность данных, предназначенная для многофункционального использования и модификации	21, 23
4	<b>Банк данных</b>	организационно-техническая <b>система</b> , включающая одну или несколько <b>баз данных</b> и систему управления ими	19
5	<b>БЕЗОПАСНОСТЬ</b>	совокупность программных, информационных и технических средств, предназначенных для централизованного сбора, хранения и коллективного использования данных об определенной предметной области человеческой деятельности, а также сами данные, которые хранятся в виде файлов или не связанных между собой <b>баз данных</b>	21, 23
6	<b>БЕЗОПАСНОСТЬ ИНФОРМАЦИИ</b>	состояние (положение) объекта (предмета, средства, процесса) при котором его характеристики (свойства, способности) и условия деятельности (протекания, проявления) сводят к минимуму эффективность деструктивного воздействия за счет наличия и успешного использования <b>систем</b> мероприятий, обеспечивающих защищенность от известных средств и методов подобного <b>воздействия</b>	32
		состояние <b>защищенности информации</b> , в том числе обрабатываемой средствами вычислительной техники, от <b>угроз</b> деструктивного воздействия	32

№	Термин	Определение понятия	Ист. <sup>1</sup>
		состояние <b>защищенности информации</b> , обрабатываемой в <b>информационных системах</b> , от внутренних или внешних <b>угроз</b> <i>Ср: «Защищенность информационной»</i>	25
7	<b>БЕЗОПАСНОСТЬ ИНФОРМАЦИОННАЯ</b>	состояние защищенности человека, общества и государства, их жизненно важных интересов от угроз деструктивного <b>воздействия</b> в <b>информационной сфере</b>	32
		состояние защищенности основных интересов личности, общества и государства в <b>информационном пространстве</b> , включая <b>информационно-телекоммуникационную инфраструктуру</b> и собственно <b>информацию</b> в отношении таких ее свойств, как целостность, объективность, <b>доступность</b> и <b>конфиденциальность</b>	4
		состояние защищенности личности, общества и государства и их интересов от <b>угроз</b> , деструктивных и иных негативных <b>воздействий</b> в <b>информационном пространстве</b>	3, 6, 15
		состояние защищенности <b>информационной среды</b> общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства	8
		состояние защищенности от внешних и внутренних <b>угроз</b> <b>информационной сферы</b> , формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства	14
		состояние защищенности интересов личности, общества и государства от <b>угроз деструктивных</b> и иных негативных <b>воздействий</b> в <b>информационном пространстве</b>	26

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>состояние защищенности, обеспечивающее <b>конфиденциальность доступа к информации</b>, авторизованный доступ к ней, ее целостность, достоверность, полноту и непротиворечивость</p> <p>«Ср: Защищенность информации»</p>	29
8	<b>Безопасность информационная</b> и коммуникационная	состояние защищенности личности, общества, государства и их интересов от существующих и потенциальных <b>угроз</b> в сфере <b>информационных и коммуникационных средств и технологий</b> , включая меры, направленные на обеспечение доступности, целостности, <b>конфиденциальности</b> и подлинности <b>информации</b>	28
9	<b>Безопасность информационная</b> международная	состояние международных отношений, исключающее нарушение мировой стабильности и создание <b>угрозы безопасности</b> государств и мирового сообщества в <b>информационном пространстве</b>	4, 6, 26, 27
10	<b>Безопасность информационная</b> и коммуникационная международная	состояние глобального <b>информационного пространства</b> , при котором исключены возможности нарушения прав личности, общества и прав государства в <b>информационной сфере</b> , а также деструктивного и противоправного воздействия на элементы национальной <b>критической информационной инфраструктуры</b>	31
		состояние международных отношений, исключающее нарушение мировой стабильности и создание <b>угрозы безопасности</b> государств и мирового сообщества в сфере <b>информационных и коммуникационных средств и технологий</b>	28

№	Термин	Определение понятия	Ист. <sup>1</sup>
11	<b>Безопасность</b> критической информационной инфраструктуры	состояние элементов <b>критической информационной инфраструктуры</b> и критической информационной инфраструктуры в целом, при котором проведение в отношении ее <b>компьютерных атак</b> не влечет за собой тяжких последствий	30
12	<b>Блокирование</b> информации	действия, следствием которых является прекращение <b>доступа к информации</b> <i>Ср.: «Искажение и подделка информации», «Модификация информации», «Преобразование информации», «Разглашение защищаемой информации», «Уничтожение информации», «Утечка информации»</i>	25
<b>В</b>			
13	<b>Владелец</b> документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена	субъект, реализующий полномочия владения, пользования и распоряжения указанными объектами в объеме, установленном <b>собственником</b>	8

№	Термин	Определение понятия	Ист. <sup>1</sup>
14	<p><b>Владелец</b> программно-технических средств, информационных ресурсов, информационных систем и информационных сетей</p>	<p>субъект <b>информационных отношений</b>, реализующий права владения, пользования и распоряжения программно-техническими средствами, <b>информационными ресурсами</b>, <b>информационными системами</b> и <b>информационными сетями</b> в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь</p>	19
15	<p><b>Владелец</b> электронных информационных ресурсов, информационных систем</p>	<p>субъект, реализующий права владения, пользования и распоряжения указанными объектами в пределах и порядке, определенных их <b>собственником</b></p> <p><i>Ср.: «Обладатель &lt;...&gt;», «Распорядитель &lt;...&gt;», «Собственник &lt;...&gt;»</i></p>	20
16	<p><b>Вмешательство</b> в информационно-телекоммуникационные системы и информационные ресурсы несанкционированное</p>	<p>вмешательство в процессы сбора, обработки, накопления, хранения, отображения, поиска, <b>распространения</b> и использования <b>информации</b> с целью нарушения нормального функционирования <b>информационных систем</b> или нарушение целостности, <b>конфиденциальности</b> и <b>доступности информационных ресурсов</b></p>	4
17	<p><b>Вмешательство</b> в информационные ресурсы несанкционированное</p>	<p>неправомерное воздействие на процессы формирования, <b>создания</b>, обработки, преобразования, <b>передачи</b>, использования, хранения <b>информации</b></p> <p>неправомерное воздействие на процессы формирования, обработки, преобразования, <b>передачи</b>, использования и хранения <b>информации</b></p> <p><i>Ср.: «Доступ к информации несанкционированный»</i></p>	6
19			26

№	Термин	Определение понятия	Ист. <sup>1</sup>
18	<b>ВОЗДЕЙСТВИЕ</b>	возбуждение (или торможение) в управляемой <b>системе</b> таких процессов, которые стимулируют желательный для управляющей стороны выбор	32
19	<b>ВОЗДЕЙСТВИЕ НА ИНФОРМАЦИЮ</b>	<b>система</b> мероприятий, оказывающих влияние на количественное или качественное (смысловое) содержание <b>информации</b> , циркулирующей в <b>информационных системах</b> , проводимых с целью преднамеренного искажения, задержки <b>распространения</b> , разрушения или уничтожения в процессе ее генерации, переработки или <b>передачи</b>	32
		действие по изменению формы предоставления и/или содержания <b>информации</b>	14, 15
20	<b>Война информационная</b>	противоборство между [двумя или более] государствами в <b>информационном пространстве</b> с целью нанесения ущерба <b>информационным системам, процессам и ресурсам</b> , критически важным [и другим] структурам, подрыва политической, экономической и социальной <b>систем</b> , а также массивной психологической обработки населения с целью дестабилизации общества и государства [а также принуждения государства к принятию решений в интересах противоборствующей стороны]	4 [6, 26, 27]
		<i>Ср.: «Конфликт военный в информационном пространстве», «Оружие информационное»</i>	
<b>Г</b>			
21	<b>Гриф секретности</b>	реквизиты, свидетельствующие о степени секретности сведений, содержащихся в носителе <b>секретной информации</b> , предоставляемые на самом носителе и (или) в сопроводительной документации на него	1

№	Термин	Определение понятия	Ист. <sup>1</sup>
<b>Д</b>			
22	<b>Данные</b>	<b>документированная информация</b> , циркулирующая в процессе ее обработки на электронно-вычислительных машинах	23
23	<b>Данные персональные</b> (информация персонального характера, информация о гражданах)	сведения или данные, позволяющие идентифицировать личность гражданина [человека] любые данные о фактах, случаях, обстоятельствах, относящиеся к физическому лицу, закрепленные на <b>материальном носителе</b> письменно или иным образом, в таком виде, который дает или может дать возможность идентифицировать личность индивидуума основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо	10 [11] 16 19
24	<b>Деятельность информационная</b>	сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность совокупность действий, направленных на удовлетворение <b>информационных потребностей субъектов информационных отношений</b>	24 24
25	<b>Документ</b>	См: « <i>Информация документированная</i> »	
26	<b>Документ электронный</b>	установленная национальным законом или стандартом доступная форма (формат) электронного представления <b>документа</b> <b>информация</b> или <b>сообщение</b> , представленные в электронной форме	11 17

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p><b>документированная информация</b>, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах</p>	22
27	<b>ДОСТУП К ИНФОРМАЦИИ</b>	возможность получения информации и [в том числе и с целью] ее [дальнейшего] использования	15, 19, 22, 26 [32]
28	<b>ДОСТУП К ИНФОРМАЦИИ несанкционированный</b>	<p><b>доступ</b> субъекта к защищаемой информации с нарушением прав или правил, установленных ее обладателем, владельцем или нормативными правовыми актами</p> <p>процесс, нарушающий принятые или установленные кем-либо правила разграничения доступа, следствием которого могут быть утечка, искажение, разрушение, уничтожение, блокирование информации, а также утрата, уничтожение или сбой функционирования носителя информации</p>	14, 15
29	<b>Доступ к информационной системе и (или) информационной сети</b>	<p>Ср.: «Вмешательство в информационные ресурсы несанкционированное»</p> <p>возможность использования информационной системы и (или) информационной сети</p>	32
30	<b>Доступ к секретной информации</b>	Санкционированный процесс ознакомления с секретной информацией физического лица, имеющего допуск к секретной информации	19
			1

№	Термин	Определение понятия	Ист. <sup>1</sup>
31	<b>Доступ</b> несанкционированный	<p><b>получение защищаемой информации</b> заинтересованным субъектом с нарушением установленных правовыми документами или собственником (владельцем) <b>информации</b> прав или правил доступа к защищаемой информации</p> <p><i>Прим.: В толковании понятий, связанных с доступом, необходимо однозначно определить, что такое собственное доступ – возможность получения информации или процесс получения/ознакомления с ней, или оба эти варианта.</i></p>	25
32	<b>Доступность</b> информации	возможность реализации беспрепятственного <b>доступа к информации</b> субъектов, имеющих на это надлежащие полномочия	14
<b>3</b>			
33	<b>ЗАЩИТА</b> <b>ИНФОРМАЦИИ</b>	<p>процесс обеспечения сохранности, целостности и надежности сведений (данных)</p> <p>деятельность, направленная на предотвращение <b>утечки защищаемой информации</b>, а также несанкционированных [и непреднамеренных] <b>воздействий</b> на нее</p> <p>деятельность, направленная на защиту прав субъектов на <b>информацию</b>, предотвращение <b>несанкционированного доступа</b> к ней и/или <b>утечки защищаемой информации</b>, несанкционированных и/или непреднамеренных воздействий на нее</p> <p>комплекс правовых, организационных и технических мер, направленных на обеспечение <b>конфиденциальности</b>, целостности, подлинности, <b>доступности</b> и сохранности информации</p>	32  11, 13, [10]  14, 15  19

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>предотвращение несанкционированного вмешательства в <b>информационные ресурсы</b>, незаконных действий по <b>получению</b>, копированию, <b>распространению</b>, искажению, уничтожению или <b>блокированию</b> информации</p>	21
		<p>принятие правовых, организационных и технических мер, направленных на обеспечение <b>защиты информации</b> от неправомерного <b>доступа</b>, уничтожения, модифицирования, <b>блокирования</b>, копирования, <b>предоставления</b>, <b>распространения</b>, а также от иных неправомерных действий в отношении такой информации; соблюдение <b>конфиденциальности информации ограниченного доступа</b>; реализацию <b>права на доступ к информации</b></p>	22
		<p>комплекс мер, обеспечивающих предотвращение <b>несанкционированного вмешательства в информационные ресурсы</b>, незаконных действий по <b>получению</b>, копированию, <b>распространению</b>, искажению, уничтожению или <b>блокированию информации</b></p>	23
		<p>комплекс мероприятий, проводимых с целью предотвращения <b>утечи</b>, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования и <b>блокирования информации</b></p>	25
		<p><i>Прим.: Данное понятие определено в подавляющем большинстве исследованных источников, при этом имеются существенные расхождения в толкованиях, в первую очередь в определяющих словах: защита информации – это деятельность, процесс, комплекс мер или их реализация.</i></p>	

№	Термин	Определение понятия	Ист. <sup>1</sup>
34	<b>Защита</b> электронных информационных ресурсов, информационных систем	комплекс правовых, организационных и технических мероприятий, направленных на их сохранение, предотвращение неправомерного <b>доступа к электронным информационным ресурсам, информационным системам</b> , включая незаконные действия по <b>получению, копированию, распространению</b> , искажению, уничтожению или <b>блокированию информации</b>	20
35	<b>ЗАЩИЩЕННОСТЬ</b> <b>ИНФОРМАЦИОННАЯ</b>	состояние элемента <b>информационной системы</b> , при котором обеспечены необходимые и достаточные условия его надежного, успешного и эффективного функционирования  <i>Прим.: В определенных, касающихся защищенности, используется преимущественно формулировка «защищенность информации», поэтому необходимо уточнение, являются ли понятия защищенности информации и информационной защищенности эквивалентными.</i>  <i>Ср.: «Безопасность информации», «Безопасность информационная»</i>	32
<b>И</b>			
36	<b>Информатизация</b>	организационный социально-экономический и научно-технический процесс, в основе которого лежит массовое применение <b>информационных систем</b> и <b>технологий</b> в целях кардинального улучшения условий труда и качества жизни населения, значительного повышения эффективности всех видов деятельности физических и юридических лиц	10
		организационный, социально-экономический и научно-технический процесс создания благоприятных условий для удовлетворения <b>информационных потребностей</b> , прав и свобод субъектов <b>информационной сферы</b>	14

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования <b>информационных ресурсов</b> и реализации <b>информационных отношений</b></p> <p>организационный, социально-экономический и научно-технический процесс, направленный на формирование и развитие электронных <b>информационных ресурсов, информационных систем</b> на основе использования <b>информационных технологий</b></p>	19
		<p>разработка, создание, освоение и использование <b>информационных технологий, информационных ресурсов</b>; процесс, включающий организационный, научно-технический, социальный и производственно-экономический компоненты и результат деятельности, направленный на удовлетворение <b>информационных потребностей</b> отдельных граждан, их объединений, государственных и негосударственных организаций, общества в целом путем формирования и использования <b>информационных ресурсов</b> во всех сферах жизни общества</p>	21, 23
37	<b>ИНФОРМАЦИЯ</b>	<p>результат (следы) взаимодействия объектов (предметов, средств) и явлений (процессов) материального мира, воспринимаемых человеком или техническими устройствами в виде сведений (данных) в различной форме представления и служащие ему источником получения, пополнения и передачи знаний (принятия решений, адаптации к изменениям окружающей среды)</p>	32

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>сведения о предметах, фактах, событиях, явлениях и процессах, касающиеся предмета договоров (контрактов), заключенных между Сторонами в ходе военно-экономического (военно-технического) сотрудничества, их исполнения и/или полученных результатах, независимо от формы их представления</p>	2
		<p>сведения о фактах, событиях, явлениях и процессах (независимо от формы их представления)</p>	7
		<p>сведения о лицах, предметах, [объектах – 21, 23], фактах, событиях, явлениях, процессах [и мнения о них – 9], независимо от формы их представления</p>	14, 15, 19, 24, [9, 21, 23]
		<p>сведения или данные, порядок использования которых независимо от способа их представления, хранения или организации подлежит правовому регулированию в соответствии с настоящим Законом и национальным законодательством</p>	10, 11, 13
		<p>сведения, представленные в любой форме и любом виде, на любых <b>носителях</b>, о лицах, предметах, фактах, событиях, явлениях и процессах, которые имели, имеют или будут иметь место в обществе, государстве и окружающей среде.</p>	12

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>полученные и оформленные в установленном законодательством порядке данные о личности, предмете, факте, обстоятельстве, событии, происшествии, явлении независимо от формы их владения или материального <b>носителя</b> (текстовые, электронные <b>документы</b>, звукозаписи, видеозаписи, фотокопии, чертежи, схемы, ноты, карты)</p> <p>сведения (<b>сообщения</b>, данные) независимо от формы их представления</p> <p>сведения об окружающем мире и протекающих в нем процессах, независимо от формы их представления</p> <p><i>Можно выделить основные элементы, составляющие определение информации:</i></p> <ol style="list-style-type: none"> <li>1. Это сведения/данные о событиях, фактах, явлениях, процессах, окружающем мире, предметах, лицах и мнения о них (могут присутствовать все элементы перечисления, или часть из них);</li> <li>2. Это сведения/данные независимо от формы их представления;</li> <li>3. Эти сведения/данные, а также их использование подлежат правовому регулированию.</li> </ol> <p><i>Данные положения используются в различных комбинациях и не всегда в полном объеме.</i></p>	18
38	<b>Информация</b> документированная (документ)	зафиксированная на <b>материальном носителе информация</b> с указанием источника ее происхождения и других реквизитов в соответствии с установленными стандартами	7

№	Термин	Определение понятия	Ист. <sup>1</sup>
		зафиксированная на <b>материальном носителе информация</b> с реквизитами, позволяющими ее идентифицировать	8, 19, 20, 21, 23
		<b>информация</b> , зафиксированная в письменной, аудиовизуальной, акустической, электронной, оптической или любой иной форме, пригодной для непосредственного восприятия, с реквизитами, установленными для данной формы <b>документа</b>	9
		<b>материальный носитель</b> с зафиксированной на нем <b>информацией</b> , который имеет реквизиты, позволяющие его идентифицировать	10
		зафиксированная на <b>материальном носителе</b> идентифицируемая <b>информация</b> , созданная, полученная и сохраняемая в качестве доказательства при подтверждении правовых обязательств или деловой деятельности	11
		сведения, представленные на любых [ <b>материальных</b> ] <b>носителях</b> в установленных законодательством форме и виде и с обязательными реквизитами, которые позволяют его идентифицировать.	12, [13]
		зафиксированная на <b>материальном носителе</b> путем документирования <b>информация</b> с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее <b>материальный носитель</b>	22
		зафиксированная на реальном <b>носителе информации</b> с реквизитами, позволяющими ее идентифицировать	24

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p><b>информация</b>, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного <b>доступа</b> на законном основании, и обладатель которой принимает меры к обеспечению ее <b>конфиденциальности</b></p> <p><b>документированная информация, доступ</b> к которой ограничивается в соответствии с законодательством</p> <p><b>информация</b>, принадлежащая на основе <b>права собственности</b>, авторского права и права на интеллектуальную собственность физическим или юридическим лицам, а также <b>информация</b>, находящаяся в собственности государства, несанкционированное разглашение и/или использование которой наносит вред физическим или юридическим лицам, обществу и государству.</p> <p><b>информация</b>, подлежащая защите в соответствии с требованиями правовых документов и/или требованиями, устанавливаемыми <b>обладателем</b> данной <b>информации</b></p> <p><b>информация, доступность</b> которой ограничена законом</p> <p><b>документированная информация</b>, доступ к которой ограничен определенным кругом лиц</p> <p>сведения, находящиеся во владении, пользовании или распоряжении отдельных физических либо юридических лиц, которые могут включаться по желанию <b>собственника</b> в состав государственных</p> <p>См.: «<i>Конфиденциальность информации</i>»</p>	<p>2</p> <p>8, 23</p> <p>12</p> <p>14, 15</p> <p>16</p> <p>21</p> <p>24</p>
39	<b>Информация</b> конфиденциальная		
40	<b>Информация</b> массовая	<p>предназначенные для неограниченного круга лиц печатные, аудиосообщения, аудиовизуальные и иные <b>сообщения</b> и материалы</p>	8

№	Термин	Определение понятия	Ист. <sup>1</sup>
		печатная, электронная (цифровая) или аудиовизуальная <b>информация</b> , опубликованная средствами массовой <b>информации</b> и предназначенная для неопределенного круга лиц.	12
41	<b>Информация</b> общедоступная	предназначенная для неопределенного круга лиц печатная, электронная (цифровая, в том числе аудио и аудиовизуальная) <b>информация</b> публично распространяемая печатная и аудиовизуальная <b>информация</b>	13
42	<b>Информация</b> ограниченного доступа (с ограниченным доступом)	<b>информация, доступ</b> к которой не ограничен <b>информация</b> , для которой установлен специальный режим хранения и использования <b>информация, доступ</b> к которой ограничен в интересах обеспечения национальной <b>безопасности</b> в соответствии с законодательством о государственной тайне, секретности и иных нормативно-правовых актов, регулирующих отношения в области защиты государственных секретов	14
43	<b>Информация</b> ограниченного пользования	<b>информация, доступ</b> к которой ограничен законодательством государств – участников СНГ либо межгосударственными договорами <b>документированная информация</b> , отнесенная к государственной тайне и <b>конфиденциальная</b>	7
		творческая <b>информация</b> , на которую распространяется авторское право и право на интеллектуальную собственность, несанкционированное использование которой наносит вред авторам этой <b>информации</b> .	9
			14, 15
			23
			12

№	Термин	Определение понятия	Ист. <sup>1</sup>
44	<p><b>Информация</b> секретная</p>	<p>сведения, выраженные в любой форме, защищаемые в соответствии с нормативными правовыми актами Сторон, переданные (полученные) в порядке, установленном законодательством каждой из Сторон и настоящим Соглашением, а также образовавшиеся в процессе сотрудничества Сторон в сфере внешнеполитической, военной, военно-технической, экономической, научно-технической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, несанкционированное <b>распространение</b> которых может нанести ущерб <b>безопасности</b> и интересам Сторон</p> <p><b>информация</b>, которая содержит сведения, составляющие государственную или другую, предусмотренную законом, тайну, несанкционированное разглашение и/или использование которой наносит вред человеку, обществу и государству.</p>	1
45	<p><b>ИНФРАСТРУКТУРА</b> <b>ИНФОРМАЦИОННАЯ</b> [инфраструктура информации]</p>	<p><b>информация</b>, которая содержит сведения, составляющие государственную или другую предусмотренную законом тайну</p> <p><b>информация</b>, содержащая государственную тайну, разглашение которой в соответствии с "Перечнем сведений, содержащих государственную тайну" наносит ущерб <b>безопасности</b> государства</p> <p>совокупность систем, средств и технологий генерации, добывания, переработки и <b>передачи информации</b>, а также систем и средств, обеспечивающих защищенность <b>информационных систем</b> и <b>информационного ресурса</b> от угроз деструктивного воздействия</p>	12
			13
			14
			32

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации</p> <p>взаимосвязанная совокупность информационных систем и подсистем</p> <p>совокупность информационных центров, баз и банков данных, систем связи и передачи данных, других структур, которые обеспечивают функционирование информационной сети государства</p> <p><i>Прим.: Это пример использования в качестве определяющего понятия не само понятие, а его содержание. В данное определение транслируется содержание понятия «информационные процессы», которое само по себе толкуется неоднозначно.</i></p> <p><i>Ср.: «Процессы информационные»</i></p>	6, 15, 26, 27
46	<b>Инфраструктура</b> информационная и коммуникационная	совокупность технических средств, систем, объектов и персонала, вовлеченных в формирование, создание, преобразование, передачу, использование и хранение информации	28
47	<b>Инфраструктура</b> информационно-коммуникационная	совокупность информационных и коммуникационных инфраструктур	29

№	Термин	Определение понятия	Ист. <sup>1</sup>
48	<b>Инфраструктура</b> информационная критическая	совокупность автоматизированных систем управления <b>критически важными объектами</b> и обеспечивающих их взаимодействие <b>информационно-телекоммуникационных сетей</b> , предназначенных для решения задач государственного управления, обеспечения обороноспособности, <b>безопасности</b> и правопорядка, нарушения (или прекращение) функционирования которых может стать причиной наступления тяжких последствий	30
		<i>Ср.: «Инфраструктура критически важная»</i>	
49	<b>Инфраструктура</b> коммуникационная	сетевая инфраструктура, обеспечивающая <b>передачу информации</b> между территориально распределенными источниками и получателями, состоящая из линий связи, использующих различные среды распространения электромагнитных сигналов, и оборудования, обеспечивающего прием, передачу этих сигналов, и их обработку в процессе этой передачи	29
50	<b>Инфраструктура</b> критически важная	объекты, системы, службы и институты, разрушение или выведение из строя которых может нанести серьезный ущерб социальному, экономическому или политическому порядку или национальной <b>безопасности</b>	28
		<i>Ср.: «Объект информационной инфраструктуры критически важный», «Структуры критически важные»</i>	
51	<b>Искажение и подделка информации</b>	изменение <b>информации</b> в результате произведенных операций по сокрытию, удалению, замене или внесению каких-либо элементов <b>информации</b> на синтаксическом, семантическом или прагматическом уровнях	25

№	Термин	Определение понятия	Ист. <sup>1</sup>
52	<b>Использование информации</b>	удовлетворение <b>информационных потребностей</b> граждан, юридических лиц и государства	24
53	<b>Использование</b> [информационно-телекоммуникационных систем и] информационных ресурсов <b>неправомерное</b>	использование [телекоммуникационных и] <b>информационных [систем и] ресурсов</b> без соответствующих прав или с нарушением установленных правил, законодательства или норм международного права	4 [6, 26]
<b>К</b>			
54	<b>КОММУНИКАЦИЯ</b>	информационный обмен, заключающийся в процессе <b>передачи</b> информации между социальным субъектом, называемым коммуникатором, и социальным объектом – коммуникантом, или группами этих социальных объектов	32
55	<b>Контроль эффективности защиты информации</b>	проверка соответствия эффективности мероприятий по <b>защите информации</b> установленным требованиям или нормам эффективности защиты  <i>Ср.: «Телекоммуникации»</i>  проверка соответствия эффективности мероприятий по <b>защите информации</b> установленным требованиям или нормам эффективности защиты  <i>Ср.: «Эффективность защиты информации»</i>	25

№	Термин	Определение понятия	Ист. <sup>1</sup>
56	<b>Конфиденциальность информации</b>	<p>требование не допускать <b>распространения</b> и (или) <b>предоставления</b> информации без согласия ее <b>обладателя</b> или иного основания, предусмотренного законодательными актами Республики Беларусь</p> <p>обязательное для выполнения лицом, получившим доступ к определенной <b>информации</b>, требование не передавать такую <b>информацию</b> третьим лицам без согласия ее <b>обладателя</b></p> <p><i>Ср.: «Информация конфиденциальная»</i></p>	19  22, 26
57	<b>Конфликт военных в информационном пространстве</b>	<p>форма разрешения межгосударственных или внутригосударственных противоречий с применением <b>информационного оружия</b></p> <p><i>Ср.: «Война информационная», «Оружие информационное»</i></p>	27
<b>М</b>			
58	<b>Модификация информации</b>	<p>изменения информации, которые требуют разрешения автора или <b>собственника информации</b></p> <p><i>Ср.: «Блокирование информации», «Искажение и подделка информации», «Разглашение защищаемой информации», «Преобразование информации», «Уничтожение информации», «Утечка информации»</i></p>	25
<b>Н</b>			
59	<b>Носители секретной информации</b>	<p>материальные объекты, в том числе физические поля, в которых <b>секретная информация</b> находит свое отображение в виде символов, образцов, сигналов, технических решений и процессов</p>	1

№	Термин	Определение понятия	Ист. <sup>1</sup>
60	<b>НОСИТЕЛЬ ИНФОРМАЦИИ</b>	любой материальный объект, в том числе физическое поле, в котором информация отображается в виде символов, образов, явлений или, например, технических решений и процессов	32
61	<b>Носитель информации</b> материальный	материал с определенными физическими свойствами, который может быть использован для записи и хранения <b>информации</b>	23
62	<b>Носитель</b> электронный	магнитный диск, магнитная лента, лазерный диск, полупроводниковые и другие <b>материальные носители</b> , используемые для регистрации и хранения <b>информации</b> электронными или иными техническими средствами	17
<b>О</b>			
63	<b>ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>	процесс, содержание которого составляет проведение единой государственной политики в виде системы мер организационно-технического, правового, социального и иного характера, адекватных <b>угрозам</b> жизненно важным интересам человека, общества и государства в <b>информационной сфере</b> система мер правового, организационно-технического и организационно-экономического характера по выявлению <b>угроз информационной безопасности</b> , предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз <i>Ср.: «Безопасность информационной»</i>	32 14, 15
64	<b>Обладатель информации</b>	физическое или юридическое лицо, общественная организация или государство, самостоятельно создавшие <b>информацию</b> , либо получившее на основании закона или договора право разрешать или ограничивать <b>доступ к информации</b>	32

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>физическое или юридическое лицо, орган государственной власти, орган местного самоуправления или судебный орган, которые своими силами создали <b>информацию</b> либо приобрели на основании закона или договора право разрешать или ограничивать <b>доступ к информации</b>, определяемой по каким-либо признакам</p> <p>субъект <b>информационных отношений</b>, получивший права <b>обладателя информации</b> по основаниям, установленным актами законодательства Республики Беларусь, или по договору</p> <p>лицо, самостоятельно создавшее <b>информацию</b> либо получившее на основании закона или договора право разрешать или ограничивать <b>доступ к информации</b>, определяемой по каким-либо признакам</p> <p><i>Ср.: «Владелец &lt;...&gt;», «Распорядитель &lt;...&gt;», «Собственник &lt;...&gt;»</i></p>	13
65	<b>Обмен</b> <b>информационный</b> международный	передача и получение <b>информационных продуктов</b> , а также оказание <b>информационных услуг</b> через государственную границу, в том числе с использованием глобальных <b>информационных сетей</b>	8
66	<b>Обслуживание</b> <b>информационное</b>	<b>информационная деятельность</b> , осуществляемая в определенной настоящей Законом форме, для доведения <b>информационной продукции</b> до пользователей с целью удовлетворения их <b>информационных потребностей</b>	24
67	<b>ОБЪЕКТ ДОСТУПА</b>	единица <b>информационного ресурса</b> , <b>доступ</b> к которому регламентируется правилами разграничения доступа	32
68	<b>ОБЪЕКТ ЗАЩИТЫ</b> <b>ИНФОРМАЦИИ</b>	<b>носитель информации</b> или <b>информационный процесс</b> , в отношении которых необходимо обеспечить защиту в соответствии с поставленной целью	32

№	Термин	Определение понятия	Ист. <sup>1</sup>
69	<b>Объект информационной инфраструктуры</b> критически важный	часть (элемент) <b>информационной инфраструктуры, воздействие</b> на которую может иметь последствия, непосредственно затрагивающие национальную <b>безопасность</b> , включая безопасность личности, общества и государства  <i>Ср.: «Инфраструктуры критически важные», «Структуры критически важные»</i>	26
70	<b>Объект инфраструктуры</b> критически важный	объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно-территориальной единицы или существованию ухудшению <b>безопасности</b> жизнедеятельности населения, проживающего на этих территориях, на длительный срок	30
71	<b>ОБЪЕКТЫ ИНФОРМАЦИОННЫЕ</b>	объекты материального мира, реализующие функции генерации (производства, воспроизводства), сбора и накопления, хранения, переработки и передачи информации  <i>Ср.: «Процессы информационные»</i>	32
72	<b>ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>	объекты материального мира, реализующие в себе функции генерации, добытия, переработки, <b>передачи информации</b> и обладающие программами реализации этих функций	32
73	<b>ОПАСНОСТЬ</b>	Опасность — свойство, внутренне <b>присущее любой сложной системе</b> . Она может реализоваться в виде прямого или косвенного ущерба.	32

№	Термин	Определение понятия	Ист. <sup>1</sup>
74	<b>Опасность</b> информационная	См. «Угроза информационной безопасности»	
75	<b>Оператор</b> информационной системы	субъект <b>информационных отношений</b> , осуществляющий эксплуатацию <b>информационной системы</b> и (или) оказывающий посредством ее <b>информационные услуги</b>  гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации <b>информационной системы</b> , в том числе по обработке <b>информации</b> , содержащейся в ее <b>базах данных</b>	19
76	<b>ОРУЖИЕ</b> <b>ИНФОРМАЦИОННОЕ</b>	Информационное оружие представляет собой совокупность средств, методов и технологий, обеспечивающих возможность силового воздействия на информационную сферу противника с целью разрушения его информационной инфраструктуры, систем управления государством, снижения обороноспособности.  средства и методы, применяемые с целью нанесения ущерба <b>информационным ресурсам, процессам и системам</b> государства, негативного информационного <b>воздействия</b> на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства, а также массивной психологической обработки населения с целью дестабилизации общества и государства	32
		<b>информационные технологии</b> , средства и методы, применяемые в целях ведения <b>информационной войны</b>	6, 15, 26, 27

№	Термин	Определение понятия	Ист. <sup>1</sup>
		<p>Ср.: «Война информационная», «Конфликт военный в информационном пространстве»</p>	
77	<p><b>Отношения</b> информационно-инфраструктурные</p>	<p>общественные отношения, возникающие в процессе <b>создания, распространения</b>, использования, сохранения и уничтожения (утилизации) информации, а также в процессе деятельности субъектов <b>информационной инфраструктуры</b>, предоставления <b>информационных услуг</b> и выполнения работ в <b>информационной сфере</b>, использования <b>информационных технологий и ресурсов</b> и обеспечения <b>информационной безопасности</b>.</p>	12, 13
		<p>отношения по поводу сбора, накопления, хранения и использования <b>информации</b></p>	7
		<p>общественные отношения, возникающие в процессе <b>создания, распространения</b>, использования, хранения и уничтожения (утилизации) <b>информации</b>.</p>	12, 13
78	<p><b>Отношения</b> информационные</p>	<p>отношения, возникающие при обработке, сборе, хранении, <b>распространении</b> и использовании <b>информации</b></p>	14
		<p>отношения, возникающие при поиске, <b>получении, передаче</b>, сборе, обработке, накоплении, хранении, <b>распространении</b> и (или) <b>предоставлении информации</b>, использовании <b>информацией, защите информации</b>, а также при применении <b>информационных технологий</b></p>	19
		<p>Ср.: «Процессы информационные»</p>	

№	Термин	Определение понятия	Ист.
<b>П</b>			
79	<b>Передача информации</b>	<i>См. «Распространение информации»</i>	
80	<b>Передача информации</b> трансграничная	передача информации оператором через государственные границы государств – участников СНГ органу власти, физическому или юридическому лицу государства	15
81	<b>Подделка информации</b>	<i>См.: «Искажение и подделка информации»</i>	
82	<b>Получение информации</b>	приобретение и накопление в соответствии с законодательством Республики Таджикистан информации о лицах, предметах, фактах, событиях, явлениях и т.д., независимо от форм их представления	24
83	<b>Пользователь</b>	субъект, обращающийся к информационной системе за получением необходимых ему электронных информационных ресурсов и пользующийся ими	20
84	<b>Пользователь</b> (потребитель) информации, средств международного информационного обмена	субъект, обращающийся к собственнику или владельцу за получением необходимых ему информационных продуктов или возможности использования средств международного информационного обмена и пользующийся ими	8
85	<b>Пользователь</b> информации	субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею	19
		субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации	24

№	Термин	Определение понятия	Ист.
86	<b>Пользователь</b> информационной системы и (или) информационной сети	субъект <b>информационных отношений</b> , получивший доступ к <b>информационной системе</b> и (или) <b>информационной сети</b> и пользующийся ими	19
87	<b>Посредник</b> информационный	субъект <b>информационных отношений</b> , предоставляющий <b>информационные услуги обладателям</b> и (или) <b>пользователям информации</b>	19
88	<b>ПОТЕНЦИАЛ</b> <b>ИНФОРМАЦИОННЫЙ</b>	возможность (способность) своевременно генерировать, добывать, перерабатывать и передавать определённые (необходимые) объёмы информации соответствующего качества. <i>Ср.: «Превосходство информационное»</i>	32
89	<b>ПОТОК</b> <b>ИНФОРМАЦИОННЫЙ</b>	генерируемая совокупность сведений ( <b>сообщений</b> , данных) независимо от формы их представления, циркулирующих в <b>системе</b> , а также между <b>системой</b> и внешней средой, предназначенный для реализации сигнальных и управляющих функций	32
90	<b>Потребитель</b> (пользователь) информационных услуг и информационных ресурсов	субъект, обращающийся к <b>информационной системе</b> , <b>собственнику информационных ресурсов</b> или <b>посреднику</b> за предоставлением ему <b>необходимой информации</b> и пользующийся ею в пределах установленных национальным законодательством или приобретенных прав <b>пользователя</b>	21, 23
91	<b>Потребность</b> <b>информационная</b>	потребность лица в <b>информации</b> для осуществления своей деятельности	10

№	Термин	Определение понятия	Ист.
92	<b>Право на доступ</b> к информации	право каждого гражданина свободно осуществлять поиск <b>информации</b> и получать ее от государственных органов и организаций, иных органов и организаций, наделенных государством властными полномочиями, органов местного самоуправления, их должностных лиц, обладающих этой <b>информацией</b> на законных основаниях	9
93	<b>Право собственности</b> на информацию	урегулированные законом общественные отношения относительно владения, пользования и распоряжения <b>информацией</b> .	12, 24
94	<b>Правонарушение</b> в информационном пространстве	См. « <i>Преступность информационная</i> »	
95	<b>ПРЕВОСХОДСТВО</b> <b>ИНФОРМАЦИОННОЕ</b>	способность более эффективно добывать, перерабатывать и распределять непрерывный <b>поток информации</b> о складывающейся в реальном масштабе времени обстановке, препятствуя противоборствующей стороне делать то же самое  Ср.: « <i>Потенциал информационный</i> »	32
96	<b>Предоставление</b> <b>информации</b>	действия, направленные на ознакомление с <b>информацией</b> определенного круга лиц  действия, направленные на <b>получение информации</b> определенным кругом лиц или <b>передачу информации</b> определенному кругу лиц  Ср.: « <i>Распространение информации</i> »	19  22, 26
97	<b>Преобразование</b> <b>информации</b>	изменения <b>информации</b> в результате операций, предписанных <b>информационной системой</b> или <b>технологией</b>	25

№	Термин	Определение понятия	Ист.
		<p><i>Ср.: «Блокирование информации», «Искажение и подделка информации», «Модификация информации», «Разглашение защищаемой информации», «Уничтожение информации», «Утечка информации»</i></p>	
98	<p><b>Преступность информационная</b> (правонарушение в информационном пространстве)</p>	<p>использование <b>информационных ресурсов</b> и (или) <b>воздействие</b> на них в <b>информационном пространстве</b> в противоправных целях</p> <p><i>Ср. «Терроризм информационный»</i></p>	6, 15, 26
99	<p><b>Преступность информационная</b> международная</p>	<p>использование <b>телекоммуникационных и информационных систем и ресурсов</b> и <b>воздействие</b> на такие системы и ресурсы в международном <b>информационном пространстве</b> в противоправных целях</p> <p><i>Ср. «Терроризм информационный международный»</i></p>	4
100	<p><b>Продукты</b> (продукция) информационные</p>	<p><b>документированная информация</b>, подготовленная в соответствии с потребностями <b>пользователей</b> и предназначенная или применяемая для удовлетворения потребностей <b>пользователей</b></p> <p>любая обособленная <b>информация</b>, представленная в конкретно организованной форме и конкретном виде, независимо от содержания, времени и места создания, по поводу которой возникают или могут возникнуть правовые отношения.</p> <p>материализованный результат <b>информационных процессов</b>, предназначенный для обеспечения <b>информационных потребностей</b> органов государственной власти, юридических и физических лиц</p>	8  12, 13  23

№	Термин	Определение понятия	Ист.
		<p>материальный результат <b>информационной деятельности</b>, предназначенный для удовлетворения <b>информационных потребностей</b> граждан, государственных органов, предприятий, учреждений и организаций</p> <p>сфера деятельности, связанная с <b>созданием, преобразованием и использованием информации</b>, включая индивидуальное и общественное сознание, <b>информационно-телекоммуникационную инфраструктуру</b> и собственную <b>информацию</b></p>	24
101	<b>Пространство информационное</b>	<p>сфера деятельности, связанная с формированием, <b>созданием, преобразованием, передачей</b>, использованием, хранением <b>информации</b>, оказывающая <b>воздействие</b> в том числе на индивидуальное и общественное сознание, <b>информационную инфраструктуру</b> и собственно <b>информацию</b></p> <p><i>Ср.: «Сфера информационная»</i></p>	6, 15, 26, 27
102	<b>ПРОЦЕССЫ ИНФОРМАЦИОННЫЕ</b>	<p>генерирование (производство), добывание, хранение, переработка и передача <b>информации</b> субъектом и функционирование естественных и технических средств в <b>информационной сфере</b></p> <p>процессы <b>создания</b>, сбора, обработки, накопления, хранения, поиска, <b>распространения</b> и потребления <b>информации</b></p> <p>процессы формирования, поиска, сбора, обработки, хранения, <b>распространения</b> и использования <b>информации</b></p> <p>процессы сбора, обработки, хранения, <b>передачи</b>, поиска и <b>распространения информации</b></p>	32  8, 20  14, 15  21, 23, 24

№	Термин	Определение понятия	Ист.
<p><i>Прим.: Понятия, связанные с информационными процессами, имеют разноточения, как и определение собственно информационных процессов. Указываются различные операции, связанные с информацией, в разных количествах и комбинациях. Для ликвидации подобных разночтений необходимо однозначно определить понятие информационных процессов, включив в него по возможности максимальный перечень подобных операций, а в определениях связанных понятий использовать термин «информационные процессы», а не его содержание.</i></p>			
<b>Р</b>			
103	<b>Работы</b> информационные	деятельность по созданию электронных <b>информационных ресурсов</b> и <b>информационных систем</b> <i>Ср.: «Услуги информационные»</i>	20
104	<b>Разглашение</b> защищаемой информации	несанкционированное доведение <b>защищаемой информации</b> до потребителей, не имеющих прав <b>доступа</b> к этой <b>информации</b> <i>Ср.: «Блокирование информации», «Искажение и подделка информации», «Модификация информации», «Преобразование информации», «Уничтожение информации», «Утечка информации»</i>	25
105	<b>Распорядитель</b> <b>информации</b>	имеющие <b>информацию</b> органы местного и государственного самоуправления, государственные учреждения, финансируемые бюджетом организации, а также организации общественного значения и их официальные лица <i>Ср.: «Владелец &lt;...&gt;», «Обладатель &lt;...&gt;», «Собственник &lt;...&gt;»</i>	18

№	Термин	Определение понятия	Ист.
		<p>деятельность, связанная с передачей <b>информации</b> от ее авторов и/или владельцев к ее потребителям.</p> <p>деятельность, связанная с <b>предоставлением информации</b> неопределенному либо определенному кругу лиц</p> <p>действия, направленные на ознакомление с <b>информацией</b> неопределенного круга лиц</p> <p>действия, направленные на получение <b>информации</b> неопределенным кругом лиц или <b>передачу информации</b> неопределенному кругу лиц</p> <p>обнародование и реализация <b>информации</b> в установленном законом порядке</p>	12 13 19 22, 26 24
106	<b>Распространение</b> (передача) информации	<i>Ср.: «Предоставление информации»</i>	
107	<b>Распространение секретной информации</b> несанкционированное	передача огласке <b>секретной информации</b> или нарушение установленного порядка (правил) <b>распространения</b> такой <b>информации</b> , вследствие чего она становится известной лицам, не имеющим допуска к ней	1
108	<b>Режим информации</b> правовой	нормативно установленные правила, определяющие степень открытости, порядок документирования, доступа, хранения, <b>распространения</b> и <b>защиты информации</b> , а также исключительные права на <b>информацию</b>	7
		установленный в соответствии с законодательством порядок <b>создания, распространения</b> , использования, хранения и уничтожения (утилизации) <b>информации</b> , а также порядок отнесения <b>информации</b> к категории <b>информации с ограниченным доступом</b>	12, 13

№	Термин	Определение понятия	Ист.
109	<b>Режим конфиденциальности</b> информации правовой	правовой режим доступа к <b>конфиденциальной информации</b> , а также регламентация порядка ее использования, способов и средств обеспечения ее защиты	12, 13
110	<b>Режим секретности</b>	установленные в государствах-Сторонах настоящего Соглашения совокупность требований, норм и правил, а также порядок применения мер, регулирующих (исключающих несанкционированный) <b>доступ к секретной информации</b>	1
111	<b>Режим секретности</b> информации правовой	правовой режим доступа к <b>секретной информации</b> , а также регламентация ее использования, способов и средств обеспечения ее защиты	12, 13
112	<b>РЕСУРСЫ ИНФОРМАЦИОННЫЕ</b>	сведения сами по себе и сведения в <b>базах данных информационных систем</b>	32
		<b>информационная инфраструктура</b> (технические средства и системы формирования, обработки, хранения и передачи информации), включая массивы и <b>базы данных</b> , собственно <b>информацию</b> и ее <b>потоки</b>	4, 14, 15
		<b>информационная инфраструктура</b> , а также собственно <b>информация</b> и ее <b>потоки</b>	6, 26, 27, 28
		отдельные <b>документы</b> и отдельные массивы документов, <b>документы</b> и массивы документов в <b>информационных системах</b> (библиотеках, архивах, фондах, <b>банках данных</b> , других видах <b>информационных систем</b> )	8
		любая совокупность <b>информации</b> , включая документы, независимо от содержания, времени и места создания.	12, 13

№	Термин	Определение понятия	Ист.
		<p>организованная совокупность <b>документированной информации</b>, включающая <b>базы данных</b>, другие совокупности взаимосвязанной <b>информации в информационных системах</b></p> <p>пригодные для использования программные средства и <b>документы</b> на любом <b>носителе</b>, отдельные либо в составе <b>информационных систем</b></p> <p><b>информация</b> независимо от способа ее представления или организации хранения (<b>документы</b>, массивы документов, фонды библиотек, архивов, <b>базы данных</b>), предназначенная для включения в <b>информационные системы</b> или содержащаяся в них</p> <p>отдельные материалы, частичный объем материалов и объем материалов в <b>информационных системах</b> (библиотеках, архивах, фондах, хранилищах сведений и других <b>информационных системах</b>)</p>	19
113	<b>Ресурс</b> <b>информационный</b> государственный	<b>информационный ресурс</b> , формируемый или приобретаемый за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц	19
114	<b>Ресурсы</b> <b>информационные</b> иностранные	<b>информационные ресурсы</b> , которые находятся под юрисдикцией иностранных государств, доступные для субъектов <b>информационных и информационно-инфраструктурных отношений</b>	12, 13
115	<b>Ресурсы</b> <b>информационные</b> конфиденциальные	<b>информационные ресурсы</b> , доступ к которым ограничен в соответствии с национальным законодательством  <i>Ср.: «Информация конфиденциальная»</i>	11
116	<b>Ресурсы</b> <b>информационные</b> международные	<b>информационные ресурсы</b> , которые находятся под юрисдикцией международного законодательства, доступные для субъектов <b>информационных и информационно-инфраструктурных отношений</b>	12

№	Термин	Определение понятия	Ист.
117	<b>Ресурсы информационных национальные</b>	<b>информационные ресурсы</b> , которые находятся под юрисдикцией государства, доступные для субъектов <b>информационных и информационно-инфраструктурных отношений</b>	12, 13
118	<b>Ресурсы информационных электронных</b>	<b>информация</b> , хранящаяся в электронном виде ( <b>информационные базы данных</b> ), содержащаяся в <b>информационных системах</b>	20
119	<b>Ресурсы информационных электронных конфиденциальные</b>	<b>электронные информационные ресурсы</b> , не содержащие государственных секретов, <b>доступ</b> к которым ограничен в соответствии с законами Республики Казахстан или их собственником либо <b>владельцем</b> в случаях, предусмотренных законодательством Республики Казахстан	20
120	<b>РИСК</b>	<b>угроза</b> или <b>опасность</b> потенциально возможной (вероятностной) потери части ресурсов или деятельности, связанная с преодолением неопределенности в ситуации выбора варианта достижения цели	32
121	<b>РИСК ИНФОРМАЦИОННЫЙ</b>	<b>угроза информационной безопасности</b> или информационная опасность потенциально возможной (вероятностной) потери части (или качества) <b>информационного ресурса</b> или деятельности, связанная с преодолением неопределенности в <b>обеспечении информационной безопасности</b>	32
<b>С</b>			
122	<b>Свобода информации</b>	осуществление права на поиск информации и ее получение от <b>распорядителя информации</b> в определенном законодательством порядке	18
123	<b>Сеть</b> информационная	совокупность <b>информационных систем</b> , взаимодействующих друг с другом по каналам связи	8

№	Термин	Определение понятия	Ист.
		совокупность <b>информационных систем</b> либо комплексов программно-технических средств <b>информационной системы</b> , взаимодействующих посредством сетей <b>электросвязи</b>	19
124	<b>Сеть</b> информационная глобальная	<b>информационная сеть</b> , обеспечивающая взаимодействие <b>информационных сетей</b> , расположенных в разных странах	8
125	<b>Сеть</b> информационно-коммуникационная	совокупность технических и аппаратно-программных средств обеспечения взаимодействия между <b>информационными системами</b> или между их составляющими, а также передачи <b>информационных ресурсов</b>	20
		совокупность технических средств для <b>передачи</b> и обработки <b>информации</b>	29
126	<b>Сеть</b> информационно-телекоммуникационная	<b>система</b> передачи данных, предназначенная преимущественно для <b>передачи информации</b> , <b>доступ</b> к которой осуществляется с использованием компьютерных и других технических устройств	10, 11
127	<b>СИСТЕМА</b>	технологическая <b>система</b> , предназначенная для передачи по линиям связи <b>информации</b> , <b>доступ</b> к которой осуществляется с использованием средств вычислительной техники	22
128	<b>СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ</b>	нечто целое, представляющее собой единство закономерно расположенных и находящихся во взаимной связи частей (элементов, предметов, явлений), объединение которых придает системе свойства, не присущие каждой из частей в отдельности	32
		целенаправленная совокупность органов и (или) исполнителей, используемой ими техники <b>защиты информации</b> , а также объектов защиты	32

№	Термин	Определение понятия	Ист.
129	<b>СИСТЕМА ИНФОРМАЦИОННАЯ</b>	<p>естественная (биологическая) или целевая (организационно-техническая) совокупность закономерно расположенных и находящихся во взаимной связи совокупность сведений об объекте (предмете, средстве, явлении, процессе), его деятельности (проявлении, протекании), а также используемые <b>информационные технологии</b></p> <p>имущественный комплекс, предназначенный для поиска, сбора, накопления, хранения, обработки и <b>передачи (распространения) информации</b> и состоящий из необходимого технического оборудования и программного обеспечения (включая <b>информацию</b>, средства ее <b>представления</b> и организации)</p> <p>организационно упорядоченная совокупность средств, реализующих определенные технологические действия посредством <b>информационных процессов</b>, предназначенных для решения конкретных функциональных задач</p> <p><b>система</b> подготовки, доставки, получения, хранения или иного типа аппаратно-программной разработки <b>электронных документов</b></p> <p>совокупность <b>банков данных, информационных технологий</b> и комплекса (комплексов) программно-технических средств</p> <p>система, предназначенная для хранения, обработки, поиска, <b>распространения, передачи и предоставления информации</b> с применением аппаратно-программного комплекса</p> <p><b>система</b>, основанная на применении <b>информационной технологии</b></p>	32  10, 11  14, 15  17  19  20  21

№	Термин	Определение понятия	Ист.
		совокупность содержащейся в <b>базах данных информации</b> и обеспечивающих ее обработку <b>информационных технологий</b> и технических средств	22, 26
		организационно упорядоченная совокупность <b>документов</b> и <b>информационных технологий</b> , в том числе с использованием средств вычислительной техники и связи, реализующих <b>информационные процессы</b>	23
		совокупность материалов, систематизированных с организационной точки зрения, объем материалов и <b>информационной технологии</b> , в том числе с использованием средств вычислительной техники и связи, предварающих <b>информационный процесс</b>	24
		<b>система</b> , предназначенная для <b>создания</b> , хранения, обработки, поиска, <b>распространения информации</b>	29
130	<b>Система</b> информационная государственная	<b>информационная система</b> , создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц	19
131	<b>Система</b> информационная межгосударственная	задействованная в межгосударственных информационных обменах <b>система</b> , принадлежащая органам СНГ, субъектам государств – участников СНГ на правах совместной собственности, совместного владения или совместного (общего) пользования	14, 15
132	<b>Система</b> информационной безопасности	комплекс мер правового, политического, организационного, кадрового, финансового, научно-технического и специального характера, нацеленный на обеспечение <b>информационной безопасности</b> государств-членов ОДКБ	3

№	Термин	Определение понятия	Ист.
133	<b>Система</b> международной информационной безопасности	совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального <b>информационного пространства</b>	31
134	<b>СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>	целенаправленная совокупность взаимосвязанных организационно-технических, правовых и социальных норм и механизмов, направленных на противодействие <b>угрозам информационной безопасности</b> с целью сведения до минимума возможного ущерба в <b>информационной сфере</b>	32
135	<b>Собственник</b> документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена	субъект, реализующий полномочия владения, пользования, распоряжения указанными объектами в объеме, устанавливаемом законом	8
136	<b>Собственник</b> информационных ресурсов, информационных систем, технологий и средств их обеспечения	субъект, владеющий и пользующийся указанными объектами и реализующий полномочия распоряжения ими в пределах, установленных законодательством	24

№	Термин	Определение понятия	Ист.
137	<b>Собственник</b> информационных ресурсов, информационных технологий, информационных систем	субъект, обладающий полномочиями владения, пользования и распоряжения указанными объектами	21, 23
138	<b>Собственник</b> программно-технических средств, информационных ресурсов, информационных систем и информационных сетей	субъект <b>информационных отношений</b> , реализующий права владения, пользования и распоряжения программно-техническими средствами, <b>информационными ресурсами, информационными системами и информационными сетями</b>	19
139	<b>Собственник</b> электронных информационных ресурсов, информационных систем	субъект, в полном объеме реализующий права владения, пользования и распоряжения электронными <b>информационными ресурсами и информационными системами</b>	20
140	<b>Создание информации</b>	Ср.: «Владелец <...>», «Обладатель <...>», «Распорядитель <...>» творческая или любая другая деятельность, результатом которой является создание <b>информационных продуктов</b> или <b>информационных ресурсов</b>	12

№	Термин	Определение понятия	Ист.
141	<b>Сообщение</b>	<b>информация</b> , посланная отправителем адресату, которая получена, зафиксирована и доступна для обработки, извлечения и восприятия в <b>информационной системе</b> адресата	11
142	<b>СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ</b>	обоснованная совокупность мероприятий и действий по <b>защите информации</b> , составляющих сущность <b>защиты информации</b> , а также определенный порядок применения <b>средств защиты информации</b> при решении конкретных задач	32
143	<b>Среда информационной</b>	См. «Сфера информационная»	
144	<b>СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b>	технические, программные, программно-технические средства, вещества и/или материалы, [а также <b>системы</b> управления комплексами средств] предназначенные или используемые для <b>защиты информации</b>	15, [32]
145	<b>Средства</b> международного информационного обмена	<b>информационные системы, сети</b> , в том числе глобальные, и сети связи, используемые при <b>международном информационном обмене</b>	8
146	<b>Структуры критически важные</b>	объекты, <b>системы</b> и институты государства, целенаправленное воздействие на <b>информационные ресурсы</b> которых может иметь последствия, прямо затрагивающие национальную <b>безопасность</b> (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, система обороны, правоохранительные органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки, объекты повышенной технической и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций)	4

№	Термин	Определение понятия	Ист.
		<p>объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную <b>безопасность</b>, включая безопасность личности, общества и государства</p> <p><i>Ср.: «Объект информационной инфраструктуры критически важный», «Инфраструктуры критически важные»</i></p>	6
147	<b>СФЕРА (СРЕДА) ИНФОРМАЦИОННАЯ</b>	<p>– (как пространство) совокупность <b>информационного ресурса, информационной инфраструктуры</b>, а также информационных объектов и субъектов, использующих <b>информацию</b>;</p> <p>– (как деятельность) связана с функционированием естественных и технических объектов (средств, предметов) генерации, распространения и <b>потребления информации</b></p> <p>сфера деятельности субъектов, связанная с <b>созданием, преобразованием и потреблением информации</b></p> <p><i>Ср.: «Пространство информационное»</i></p>	32
		<b>Т</b>	
148	<b>Телекоммуникации</b> (электросвязь)	<p>любая передача, излучение или прием знаков, сигналов, письменного текста, изображений и звуков или <b>сообщений</b> любого рода по проводной, радио-, оптической или другим электромагнитным системам</p> <p>связь с помощью электромагнитных колебаний вне зависимости от среды распространения</p> <p><i>Ср.: «Коммуникация»</i></p>	5  29

№	Термин	Определение понятия	Ист.
149	<b>Терроризм</b> <b>информационный</b> (терроризм в информационном пространстве)	использование <b>информационных ресурсов</b> и (или) воздействие на них в <b>информационном пространстве</b> в террористических целях  <i>Ср.: «Преступность информационная»</i>	6, 15, 26
150	<b>Терроризм</b> <b>информационный</b> международный	использование <b>телекоммуникационных и информационных систем и ресурсов</b> и воздействие на такие системы и ресурсы в международном <b>информационном пространстве</b> в террористических целях  <i>Ср.: «Преступность информационная международная»</i>	4
151	<b>Технологии</b> информационно-коммуникационные	<b>информационные процессы</b> и методы работы с <b>информацией</b> , осуществляемые с применением средств вычислительной техники и средств <b>телекоммуникации</b>  совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью формирования, <b>преобразования, передачи, использования и хранения информации</b>  технологии, предназначенные для совместной реализации <b>информационных и коммуникационных процессов</b>	15  26  29
152	<b>Технологии</b> информационные	организованная совокупность процессов, элементов, устройств или методов, используемых для обработки <b>информации</b>  методы и способы поиска, сбора, хранения, обработки и <b>передачи (распространения) информации</b> на основе использования компьютерных и других технических устройств, программ для электронных вычислительных машин и средств связи	7  10, 11

№	Термин	Определение понятия	Ист.
		<p>совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, <b>передачу, распространение и защиту информации</b></p> <p>совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, <b>распространения и (или) предоставления информации</b>, а также пользования <b>информацией и защиты информации</b></p> <p>совокупность средств вычислительной техники и <b>телекоммуникаций</b>, программных средств и методов их использования для поиска, обработки, хранения, <b>передачи и получения информации</b></p> <p>процессы, методы поиска, сбора, хранения, обработки, <b>предоставления, распространения информации</b> и способы осуществления таких процессов и методов</p> <p><i>Прим.: Определение в большинстве своем похоже (технологии определяется как совокупность средств, процессов и методов), а различия определяются в первую очередь неоднозначным толкованием информационных процессов: в различных определениях используется различный набор операций, связанных с информацией.</i></p> <p><i>Ср.: «Процессы информационные»</i></p>	15, 20  19  21, 23  22, 29
153	<b>Технологии</b> коммуникационные	процессы и методы <b>передачи информации</b> и способы их осуществления	29

№	Термин	Определение понятия	Ист.
154	<b>Технологии</b> информационно-телекоммуникационные (информационно-коммуникационные)	совокупность методов и способов поиска, сбора, хранения, обработки и передачи (распространения) <b>информации, доступ</b> к которой и <b>передача</b> которой осуществляются с использованием <b>информационно-телекоммуникационной сети</b>	11
<b>У</b>			
155	<b>УГРОЗА</b>	возможность возникновения совокупности факторов и условий, создающих <b>опасность</b> нанесения ущерба жизненно важным интересам человека, общества и государства	32
156	<b>УГРОЗА</b> <b>ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b> (угроза в информационном пространстве, информационная опасность)	информационная <b>опасность</b> , реализация которой становится весьма вероятной, фактор или совокупность факторов, создающих <b>опасность</b> функционированию и развитию информационной среды общества. факторы, создающие <b>опасность</b> основным интересам личности, общества и государства в <b>информационном пространстве</b>	32 4 6, 15, 26
157	<b>Угроза</b> информационной и коммуникационной безопасности	совокупность условий и факторов, создающих <b>опасность</b> нанесения ущерба интересам государств – участников СНГ в <b>информационной сфере</b>  факторы, создающие опасность для личности, общества, государства и их интересов в <b>информационном пространстве</b>	14  28

№	Термин	Определение понятия	Ист.
158	<b>Уничтожение информации</b>	умышленное или неосторожное действие, вследствие которого <b>информация</b> перестает существовать для юридических или физических лиц в полном или ограниченном объеме  <i>Ср.: «Блокирование информации», «Искажение и подделка информации», «Модификация информации», «Преобразование информации», «Разглашение защищаемой информации», «Утечка информации»</i>	25
159	<b>Услуги информационные</b>	действия субъектов (собственников и владельцев) по обеспечению <b>пользователей информационными продуктами</b> предоставление исполнителем в соответствии с его полномочиями или функциями <b>информации</b> получателю этой услуги  деятельность по обеспечению оборота <b>информации</b> , направленная на удовлетворение <b>информационных потребностей</b> субъектов <b>информационных отношений</b> , осуществляемая как на договорной, так и на не договорной основе.  деятельность по осуществлению поиска, получения, передачи, сбора, обработки, накопления, хранения, <b>распространения</b> и (или) <b>предоставления информации</b> , а также <b>защиты информации</b> услуга по предоставлению пользователям <b>информационных ресурсов</b>  услуги, направленные на удовлетворение <b>информационных потребностей</b> граждан и организаций, предоставляемые физическими и юридическими лицами, занятыми в <b>информационной сфере</b>	8  11  12, 13  19  20  21, 23

№	Термин	Определение понятия	Ист.
		<p><i>Прим.: В некоторых актах наравне с понятием «услуги» используется также понятие «работы»</i></p> <p><i>Ср.: «Работы информационных»</i></p>	
160	<b>Утечка информации</b>	<p>неконтролируемое распространение <b>защищаемой информации</b> [в результате <b>несанкционированного доступа</b>]</p> <p><i>Ср.: «Блокирование информации», «Искажение и подделка информации», «Модификация информации», «Преобразование информации», «Разглашение защищаемой информации», «Уничтожение информации»</i></p>	14, [25]
<b>X</b>			
161	<b>Хранение информации</b>	<p>обеспечение надлежащего состояния <b>информации</b>, ее <b>материальных носителей</b> и их учет</p>	24
<b>Э</b>			
162	<b>Электросвязь</b>	<p><i>См. «Телекоммуникации»</i></p>	
163	<b>Эффективность защиты информации</b>	<p>степень соответствия достигнутых результатов действий по <b>защите информации</b> поставленным целям защиты</p> <p><i>Ср.: «Контроль эффективности защиты информации»</i></p>	25

## **ПЕРЕЧЕНЬ НОРМАТИВНЫХ ИСТОЧНИКОВ, ИСПОЛЬЗОВАННЫХ ПРИ СОСТАВЛЕНИИ СЛОВАРЯ-СПРАВОЧНИКА**

1. Соглашение о взаимном обеспечении сохранности секретной информации в рамках ОДКБ (Астана, 18.06.2004 г.)
2. Соглашение о взаимной охране прав на результаты интеллектуальной деятельности, полученные и используемые в ходе военно-экономического сотрудничества в рамках ОДКБ (Душанбе, 06.10.2007 г.)
3. Положение о сотрудничестве государств-членов ОДКБ в сфере обеспечения информационной безопасности от 10.12.2010 г.
4. Доклады генерального секретаря ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» A/54/213 от 9.06.1999 г. и A/55/140 от 12.05.1999 г.
5. Регламент радиосвязи (документ Международного союза электросвязи), версия 2012 г.
6. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности от 02.12.2008 г.
7. Модельный закон МПА СНГ «О принципах регулирования информационных отношений в государствах – участниках СНГ» от 23.05.1993 г.
8. Модельный закон МПА СНГ «О международном информационном обмене» от 26.03.2002 г.
9. Модельный закон МПА СНГ «О праве на доступ к информации» от 17.04.2004 г.
10. Модельный закон МПА СНГ «Об информатизации, информации и защите информации» от 18.11.2005г.
11. Модельный закон МПА СНГ «Об электронных государственных услугах» от 7.04.2010 г.
12. Модельный информационный кодекс МПА СНГ от 3.04.2008 г.
13. Модельный информационный кодекс МПА СНГ от 23.11.2012 г.
14. Концепция сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности от 10.10.2008 г.
15. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20.11.2013 г.
16. Закон Республики Армения №3Р-492 «О персональных данных» от 7.11.2002 г.
17. Закон Республики Армения «Об электронном документе и электронной цифровой подписи» от 14.12.2004 г.

18. Закон Республики Армения №ЗР-11 «О свободе информации» от 23.09.2003 г.
19. Закон Республики Беларусь № 455-3 «Об информации, информатизации и защите информации» от 10.11.2008 г.
20. Закон Республики Казахстан № 217-III «Об информатизации» от 11.01.2007 г.
21. Закон Кыргызской Республики № 107 «Об информатизации» от 08.10.1999 г.
22. Федеральный закон Российской Федерации №149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г.
23. Закон Республики Таджикистан № 40 «Об информатизации» от 06.08.2001 г.
24. Закон Республики Таджикистан № 55 «Об информации» от 10.05.2002 г.
25. Закон Республики Таджикистан № 71 «О защите информации» от 02.12.2002 г.
26. Концепция Конвенции об обеспечении международной информационной безопасности (представлена 21-22 сентября 2011 г.).
27. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве (Министерство обороны России, 2011 г.)
28. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности от 14.05.2010 г.
29. Глоссарий (термины и определения) к проекту Концепции развития информационно-коммуникационной инфраструктуры и технологий в Российской Федерации (Министерство связи России)
30. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.
31. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.
32. Материалы исследований понятийного аппарата сферы информационной безопасности, опубликованные авторами в журнале «Информатизация и связь» (2010-2014 гг.).

## АЛФАВИТНЫЙ УКАЗАТЕЛЬ

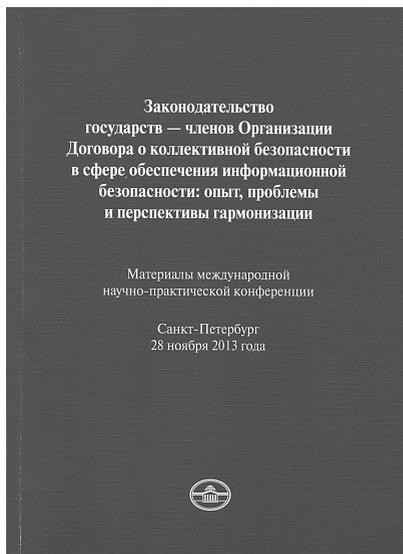
<p><b>А</b>.....36</p> <p>Автоматизация</p> <p>Атака компьютерная</p> <p><b>Б</b>.....36</p> <p><b>БАЗА ДАННЫХ</b></p> <p>Банк данных</p> <p><b>БЕЗОПАСНОСТЬ</b></p> <p><b>БЕЗОПАСНОСТЬ ИНФОРМАЦИИ</b></p> <p><b>БЕЗОПАСНОСТЬ ИНФОРМАЦИОННАЯ</b></p> <p>Безопасность информационная и коммуникационная</p> <p>Безопасность информационная международная</p> <p>Безопасность информационная и коммуникационная международная</p> <p>Безопасность критической информационной инфраструктуры</p> <p>Блокирование информации</p> <p><b>В</b>.....40</p> <p>Владелец документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена</p>	<p>Владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей</p> <p>Владелец электронных информационных ресурсов, информационных систем</p> <p>Вмешательство в информационно-телекоммуникационные системы и информационные ресурсы несанкционированное</p> <p>Вмешательство в информационные ресурсы несанкционированное</p> <p><b>ВОЗДЕЙСТВИЕ</b></p> <p><b>ВОЗДЕЙСТВИЕ НА ИНФОРМАЦИЮ</b></p> <p>Война информационная</p> <p><b>Г</b>.....42</p> <p>Гриф секретности</p> <p><b>Д</b>.....43</p> <p>Данные</p> <p>Данные персональные (информация персонального характера, информация о гражданах)</p> <p>Деятельность информационная</p>
---	--

Документ	Информация ограниченного пользования
Документ электронный	Информация секретная
<b>ДОСТУП К ИНФОРМАЦИИ</b>	<b>ИНФРАСТРУКТУРА ИНФОРМАЦИОННАЯ</b>
<b>ДОСТУП К ИНФОРМАЦИИ</b>	(инфраструктура информатизации)
<b>НЕСАНКЦИОНИРОВАННЫЙ</b>	Инфраструктура информационная и коммуникационная
Доступ к информационной системе и (или) информационной сети	Инфраструктура информационно-коммуникационная
Доступ к секретной информации	Инфраструктура информационная критическая
Доступ несанкционированный	Инфраструктура коммуникационная
Доступность информации	Инфраструктура критически важная
<b>З</b> .....45	Искажение и подделка информации
<b>ЗАЩИТА ИНФОРМАЦИИ</b>	Использование информации
Защита электронных информационных ресурсов, информационных систем	Использование [информационно-телекоммуникационных систем и] информационных ресурсов неправомерное
<b>ЗАЩИЩЕННОСТЬ ИНФОРМАЦИОННАЯ</b>	<b>К</b> .....57
<b>И</b> .....47	<b>КОММУНИКАЦИЯ</b>
Информатизация	Контроль эффективности защиты информации
<b>ИНФОРМАЦИЯ</b>	Конфиденциальность информации
Информация документированная (документ)	Конфликт военный в информационном пространстве
Информация конфиденциальная	<b>М</b> .....58
Информация массовая	Модификация информации
Информация общедоступная	
Информация ограниченного доступа (с ограниченным доступом)	

Н.....	58	Отношения информационно-инфраструктурные
<b>НОСИТЕЛЬ ИНФОРМАЦИИ</b>		Отношения информационных
Носители секретной информации		П.....
Носитель информации материальный		Передача информации
Носитель электронный		Передача информации трансграничная
О.....	59	Подделка информации
<b>ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>		Получение информации
Обладатель информации		Пользователь
Обмен информационный международный		Пользователь (потребитель) информации, средств международного информационного обмена
Обслуживание информационное		Пользователь информации
<b>ОБЪЕКТ ДОСТУПА</b>		Пользователь информационной системы и (или) информационной сети
<b>ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ</b>		Посредник информационный
Объект информационной инфраструктуры критически важный		<b>ПОТЕНЦИАЛ ИНФОРМАЦИОННЫЙ</b>
Объект инфраструктуры критически важный		<b>ПОТОК ИНФОРМАЦИОННЫЙ</b>
<b>ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>		Потребитель (пользователь) информационных услуг и информационных ресурсов
<b>ОПАСНОСТЬ</b>		Потребность информационная
Опасность информационная		Право на доступ к информации
Оператор информационной системы		Право собственности на информацию
<b>ОРУЖИЕ ИНФОРМАЦИОННОЕ</b>		Правонарушение в информационном пространстве
		<b>ПРЕВОСХОДСТВО ИНФОРМАЦИОННОЕ</b>

Предоставление информации	
Преобразование информации	
Преступность информационная	
(правонарушение в информационном пространстве)	
Преступность информационная международная	
Продукты (продукция) информационные	
Пространство информационное	
<b>ПРОЦЕССЫ ИНФОРМАЦИОННЫЕ</b>	<b>Р.....69</b>
Работы информационные	
Разглашение защищаемой информации	
Распорядитель информации	
Распространение (передача) информации	
Распространение секретной информации несанкционированное	
Режим информации правовой	
Режим конфиденциальности информации правовой	
Режим секретности	
Режим секретности информации правовой	
<b>РЕСУРСЫ ИНФОРМАЦИОННЫЕ</b>	
Ресурс информационный государственный	
Ресурсы информационные иностранные	
Ресурсы информационные конфиденциальные	
Ресурсы информационные международные	
Ресурсы информационные национальные	
Ресурсы информационные электронные	
Ресурсы информационные электронные конфиденциальные	
<b>РИСК</b>	
<b>РИСК ИНФОРМАЦИОННЫЙ</b>	<b>С.....73</b>
Свобода информации	
Сеть информационная	
Сеть информационная глобальная	
Сеть информационно-коммуникационная	
Сеть информационно-телекоммуникационная	
<b>СИСТЕМА</b>	
<b>СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ</b>	
<b>СИСТЕМА ИНФОРМАЦИОННАЯ</b>	
Система информационная государственная	
Система информационная межгосударственная	
Система информационной безопасности	
Система международной информационной безопасности	
<b>СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>	
Собственник документированной информации, информационных ресурсов, информационных	

продуктов и (или) средств международного информационного обмена	Терроризм информационный международный
Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения	Технологии информационно-коммуникационные
Собственник информационных ресурсов, информационных технологий, информационных систем	Технологии коммуникационные
Собственник программно-технических средств, информационных систем и информационных сетей	Технологии информационно-телекоммуникационные (информационно-коммуникационные)
Собственник электронных информационных ресурсов, информационных систем	Угроза информационной и коммуникационной безопасности
Создание информации	Уничтожение информации
Сообщение	Услуги информационные
<b>СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ</b>	Утечка информации
Среда информационная	Х.....85
<b>СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b>	Хранение информации
Средства международного информационного обмена	Э.....85
Структуры критически важные	Электросвязь
<b>СФЕРА (СРЕДА) ИНФОРМАЦИОННАЯ</b>	Эффективность защиты информации
Т.....80	



**Законодательство государств – членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации:** Материалы международной научно-практической конференции (Санкт-Петербург, 28 ноября 2013 г.) / Под ред. П.П. Рябухина, В.В. Бондуrowsкого, Г.И. Перекопского. – СПб.: Секретариат Совета Межпарламентской Ассамблеи государств – участников СНГ. 2014. **ISBN 978-5-86857-054-4**

*Участники конференции констатировали, что согласование законодательной политики, скоординированные меры по сближению и унификации национальных законодательств государств – членов ОДКБ в информационной сфере, обеспечение соответствия национальных законодательств международным договорам будут отвечать интересам государств – членов ОДКБ в защите конституционного строя, обеспечении суверенитета, территориальной целостности, политической, экономической и социальной стабильности. Взаимопониманию и конструктивному сотрудничеству будут способствовать легитимность и единство легальных лексических форм.*



**Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ. Сборник / Сост.: Бачило И.Л., Вус М.А., Гусев В.С., Макаров О.С. – СПб.: СПИИРАН, изд-во «Анатолия». – СПбОНТЗ, «Полиграф-экспресс». – 2011. – 79 с. ISBN 978-5-7452-0026-7.**

Сборник адресован работникам законодательных и исполнительных органов власти, руководителям и специалистам в сфере защиты государственной тайны, практическим и научным работникам, преподавателям учебных заведений, курсантам. Материал глоссария может быть использован как учебно-справочное пособие в системе подготовки и повышения квалификации кадров.



**Словарь-справочник терминов и определений понятий модельного законодательства государств – участников СНГ /** Сергеев А.И., Александрова О.А., Кучерявый М.М., Подкидышева В.Е. и др. // Под ред. М.А. Вуса и В.В. Бондуrowsкого. – СПб.: Издательство «Юридический Центр-Пресс», 2012. – 360 с. **ISBN 978-5-94201-644-9**

Содержание Словаря-справочника составляют значения и разъяснения терминов (понятий), содержащихся в принятых МПА СНГ актах модельного законодательства. Словарь включает более 3200 легальных определений понятий, приводимых в законодательных актах.

*Работа авторского коллектива была отмечена профессиональной премией – Дипломом Национального Форума по информационной безопасности «ИНФОФОРУМ – 2013».*

**Научно-практическое издание**

*Вус Михаил Александрович  
Кучерявый Михаил Михайлович  
Подкидышева Валерия Евгеньевна  
Шакин Дмитрий Николаевич  
Юсупов Рафаэль Мидхатович*

**ISBN 978-5-7452-0050-2**



**СЛОВАРЬ – СПРАВОЧНИК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
ДЛЯ ПАРЛАМЕНТСКОЙ АССАМБЛЕИ ОДКБ**

Набор, корректура рукописи – Е.М. Денисова

199178, Россия, Санкт-Петербург, 14 линия, 39  
Санкт-Петербургский институт информатики и автоматизации РАН  
E-mail: [spiiran@iiias.spb.su](mailto:spiiran@iiias.spb.su)

---

Подписано в печать 17.07.2014. Формат 60x90 1/16  
Бумага офсетная, Усл. печ. л. 5,9. Тираж 200 экз.  
Оригинал-макет подготовлен в СПбОНТЗ  
Отпечатано с оригинал-макета  
в типографии «Полиграфические технологии»  
СПб, ул. Курчатова, д.9, тел. +7 (812) 297-48-97



**ISBN 978-5-7452-0050-2**