ЗИ Защита информации

ЗИ.8 Терминология в сфере международной информационной безопасности (число стр. - 10)

В настоящее время в области обеспечения международной информационной безопасности используется большое количество схожих терминов, зачастую не имеющих общепризнанного определения

Наиболее острые дискуссии на международных площадках в сфере международной информационной безопасности (МИБ) разворачиваются вокруг трактовки терминов «cybersecurity» и «information security» и связанных с ними смысловых нюансов. В статье проведен анализ базовых определений и их трактовки в национальной и международной правовых базах.

1. ТЕРМИН БЕЗОПАСНОСТЬ ИНФОРМАЦИИ (INFORMATION SECURITY)

В соответствии с ГОСТ Р 50922–2006 «Защита информации. Основные термины…», «безопасность информации (данных) — состояние защищённости информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность» [1].

Безопасность информации, таким образом, определяется как защищённость информации от внутренних и внешних угроз: от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п.; от случайных или преднамеренных несанкционированных воздействий на информацию или несанкционированного её получения; от случайного или преднамеренного доступа лиц, не имеющих права на получение информации, её раскрытие, и др.

Термин «безопасность информации (данных)» существует не только в российской терминологии.

Он применяется в глоссарии NIST [2], в глоссарии международного стандарта безопасности данных индустрии платежных карт PCI DSS, в стандарте ISO/IEC 27000:2012 [3], в международном электротехническом словаре (IEV ref 721–08–57), разработанном Международным союзом электросвязи, а также в документах стратегического планирования ряда иностранных государств, например, в стратегии кибербезопасности Финляндии [4].

Фактически термин «безопасность информации» одинаково определяется как в России, так и за рубежом, и означает обеспечение защиты информации, т. е. её целостности, доступности и конфиденциальности.

2. ТЕРМИН «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

В начале 1990-х годов термин «информационная безопасность» начал появляться в политологических работах, и обозначаемая им сфера

отношений понималась как антипод информационной войны. При этом сама информационная война рассматривалась, в основном, как межгосударственное противоборство [5].

В то же время, часто этот термин не вполне корректно используется как синоним термина «безопасность информации».

В Доктрине информационной безопасности Российской Федерации под информационной безопасностью Российской Федерации понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Понятия «информационная безопасность» и «безопасность информации» взаимосвязаны. Слово «информационная» в термине «информационная безопасность» указывает на направление деятельности, которая может причинить вред объекту защиты. В этом случае понятие «информационная безопасность» определяется как состояние защищённости данного объекта от угроз информационного характера. При этом объектом защиты может быть не только информация, но и человек.

В литературе под информационной безопасностью также понимается состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиту субъектов информационных отношений от негативного информационного воздействия [6].

При этом «информационная среда» была определена [7] как сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Таким образом, термин «информационная безопасность» является более широким и включает в себя кроме безопасности информации (данных) также и защиту субъектов информационных отношений от негативного информационного воздействия.

Следует отметить, что при буквальном переводе на английский язык без учета контекста термин «информационная безопасность», как и термин «безопасность информации» переводятся одинаково — «information security».

В связи с этим некорректное понимание термина «информационная безопасность» встречается и в нормативной правовой базе Российской Федерации. Так, в соответствии с ГОСТ Р ИСО/МЭК 17799–2005 (перевод стандарта ISO/IEC 17799:2005) под информационной безопасностью понимается защита конфиденциальности, целостности и доступности информации. Фактически данный ГОСТ безопасность информации

определяет как «информационную безопасность». По нашему мнению, это вызвано некорректным переводом с английского языка на русский термина «information security», который необходимо было перевести как «безопасность информации».

3. ТЕРМИН «КИБЕР» («CYBER»)

В западной практике широко используется термин «cybersecurity» (кибербезопасность).

Исторические данные свидетельствуют, что слово «кибернетика» (от греческого — «кормчий») применялось ещё до нашей эры — для обозначения искусства управления кораблём или колесницей. Новое понимание слова предложил в 1830-х годах Андре Ампер, определив кибернетику как науку об управлении государством. В 1950-х годах термин был вновь введён в научный оборот Норбертом Винером как наука об общих закономерностях процессов управления, передачи и обработки информации в машинах, живых организмах и обществе, изучающая особенности обратной связи.

На основе термина «кибернетика» в 1984 году Уильям Гибсон конструирует и использует в романе «Нейромант» термин «киберпространство» (Cyberspace), под которым понималось цифровое пространство компьютерных сетей. Это слово получило широкое распространение и породило множество других слов с приставкой cyber.

Рассмотрим современные определения производных от этого слова терминов.

МСЭ утвердила следующее определение [8]: «Кибербезопасность — это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде.

Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее: доступность; целостность, которая может включать аутентичность и неотказуемость; конфиденциальность».

В соответствии с определением международного стандарта ISO [9], под

кибербезопасностью понимают обеспечение конфиденциальности, целостности и доступности в киберпространстве. При этом под киберпространством понимают комплексную среду, которая не существует ни в какой физической форме, сформированную в результате действий людей, программ и сервисов в сети интернет с использованием подключенных устройств и сетей.

В стратегии кибербезопасности Новой Зеландии значится: «Кибербезопасность — практика создания сетей, составляющих киберпространство, насколько возможно защищенных от вторжений, поддерживающих конфиденциальность, целостность и доступность информации, обнаружение происходящих вторжений и инцидентов, реагирования и восстановления после них». При этом под киберпространством понимается «глобальная сеть взаимосвязанных информационных инфраструктур, телекоммуникационных сетей, компьютерных систем обработки данных, в которых происходит обмен данными в режиме реального времени (онлайн)».

В соответствии с определением Национального комитета по системам безопасности США [10], «кибербезопасность: возможность защищать и оборонять использование киберпространства от кибератак». При этом «киберпространство» — глобальная информационная сфера, состоящая из взаимозависимых инфраструктур информационных систем (включая интернет), телекоммуникационных сетей, компьютерных систем и встраиваемых процессоров и контроллеров.

Следует обратить внимание на использование в приведённом определении понятия «оборона» (defend). Этим словом обозначается вид боевых действий, который предполагает, в том числе, проведение контратак.

Можно отметить, что единое понимание термина «cybersecurity» отсутствует. В документах ISO оно используется как эквивалент термина «безопасность информации», и не включает в себя безопасность критической информационной инфраструктуры и физическую безопасность устройств. Тогда как определение в МСЭ подразумевает безопасность устройств и «ресурсов организации», к которым, в частности относятся и критические информационные инфраструктуры.

Тем не менее, можно сделать вывод, что понятие «cybersecurity» схоже с определением термина «безопасность информации», за исключением нормативной базы США, где дополнительно используется понятие «оборона».

4. ИСПОЛЬЗОВАНИЕ ТЕРМИНОЛОГИИ В СФЕРЕ МИБ НА МЕЖДУНАРОДНЫХ ПЛОЩАДКАХ

США и их союзники стремятся сохранить и приумножить свои возможности организовывать масштабные операции в информационном пространстве иностранных государств, и не допустить наложения никаких ограничений на их проведение с использованием международного права.

Для этого США на всех международных площадках продвигают в сфере МИБ два основных тезиса:

- достаточность существующей нормативной правовой базы в отношении применения информационного оружия;
- возможность применения ими информационного оружия в любой момент — в зависимости от возникающих целей (экономических, политических и иных).

Противопоставленный данной позиции подход Российской Федерации на международной арене в сфере МИБ заключается в следующем:

- необходимость введения чёткого нормативного регулирования вопросов использования информационных и коммуникационных технологий (ИКТ), включая вопросы безопасности, отражающего современное состояние развития ИКТ;
- противодействие милитаризации информационного пространства;
- противодействие легализации использования ИКТ в ущерб третьим странам.

При этом в международной практике западными странами используется термин «кибербезопасность», а термин «безопасность информации» практически не применяется.

Формально возможность проведения ответных и превентивных компьютерных атак в явном виде не закреплена ни в одном международном правовом акте. Однако такие атаки могут трактоваться как один из способов обеспечения «кибербезопасности». Таким образом, применение термина «кибербезопасность» фактически легализует данную деятельность.

Пользуясь тем, что данные термины могут восприниматься как тождественные, как синонимы, в США замалчивают тот факт, что американская трактовка термина «кибербезопасность» включает в себя не только защиту, но и оборону. Получается, что понятие «кибербезопасность» включает использование компьютерных атак для осуществления ответных воздействий на информационную инфраструктуру, в том числе расположенную на территории иностранных государств.

Данный вывод подтверждается исследованиями компании Gartner. В 2013

году в статье Definition: Cybersecurity отмечено, что «использование термина cybersecurity в качестве синонима "безопасности информации" или "безопасности ИТ" вводит клиентов и специалистов по безопасности в заблуждение, а также размывает критические различия между этими дисциплинами» [11].

Экспертами Gartner предложено следующее определение: «В понятие "кибербезопасность" входит широкий спектр практических приемов, инструментов и концепций, тесно связанных с технологиями информационной и операционной безопасности. Отличительная черта кибербезопасности заключается в том, что она включает в себя использование информационных технологий в наступательных целях для атаки противника» [12].

Данная трактовка определений совпадает с позицией США и их союзников, предусматривающей использование информационного оружия. Ими продвигается тезис о том, что конфликты в информационном пространстве предотвратить невозможно, поэтому международное право должно их только регулировать. При этом основным механизмом такого регулирования должно стать существующее международное гуманитарное право. Так, в выпущенном в 1999 году и переизданном в 2000 году документе Пентагона сказано, что «в настоящее время в международном праве не существует никаких ограничителей на проведение информационных операций» [13].

Следует отметить, что в нормативных актах Минобороны США [14] получение несанкционированного доступа к информационным системам иностранных государств, в том числе с применением технологий бот-сетей, относится к оборонительным операциям.

5. ТЕРМИН «БЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ ИКТ И САМИХ ИКТ»

Учитывая изложенные наблюдения, использование термина «кибербезопасность» для Российской Федерации является неприемлемым.

С другой стороны, использование термина «information security» не принимается США и их союзниками. Западные эксперты отказываются от использования данного термина под предлогом того, что это позволит «недемократическим» режимам «санкционировать цензуру» и легализовать наступление на право граждан на свободное выражение мнения в сети интернет.

В этих условиях экспертами Российской Федерации в 2010 году [15] был предложен компромиссный термин «безопасность при использовании ИКТ и самих ИКТ». Термин был согласован правительственными экспертами ряда стран-членов ООН, включая США.

Данный термин с тех пор активно применяется в современном международном праве. В частности, он используется в профильных резолюциях ООН, решениях ОБСЕ, совместном заявлении Президентов Российской Федерации и Соединённых Штатов Америки о мерах укрепления доверия в сфере использования ИКТ, концепции Конвенции о международной информационной безопасности и т.д.

В указанной концепции Конвенции под ИКТ понимается «совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью формирования, преобразования, передачи, использования и хранения информации».

Фактически термин «безопасность при использовании ИКТ и самих ИКТ» шире термина «безопасность информации», и может трактоваться как синоним термина «информационная безопасность».

Следует отметить, что в отечественной нормативной базе данный термин практически не применяется, а его определение отсутствует.

6. ВЫВОДЫ

Таким образом, термин «кибербезопасность» (cybersecurity) в целом совпадает с термином «безопасность информации» (information security), но подразумевает возможность проведения компьютерных атак на информационную инфраструктуру иностранных государств.

Использование данного термина в международном праве позволяет США и их союзникам легализовать проведение информационных операций против третьих стран. В связи с чем закрепление термина «кибербезопасность» в нормативных международных правовых актах и правовых актах Российской Федерации следует признать недопустимым.
В качестве альтернативы в международном праве необходимо отстаивать использование применяемого в последнее время в международных документах, в том числе в документах ООН, термина «безопасность при использовании ИКТ и самих ИКТ», а в национальном законодательстве применять термины «безопасность информации» и «информационная безопасность».

ЛИТЕРАТУРА

1. *ГОСТ Р 50922-2006 «Защита информации. Основные термины...»*
2. *NIST Glossary of Key Information Security Terms (SP 800-66)*
3. *ISO/IEC 27000:2012 Information technology Security techniques – Information security management systems – Overview and vocabulary*
4. *Finland´s Cyber security Strategy*
5. *Александр Федоров,* http://www.pircenter.org/media/content/files/10/13559195650.pdf
6. *Алексеенцев А.И. Сущность и соотношение понятий «защита информации» и «безопасность информации» // «Безопасность информационных технологий», № 1, 1999*
7. *ФЗ «Об участии в международном информационном обмене» от 4.07.1996 №85-ФЗ*
8. *Рекомендация МСЭ-Т X.1205, 2010, Резолюция 181 Конференции в Гвадалахаре.*
9. *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity*
10. *CNSS Instruction No 4009*
11. *Definition: Cybersecurity, 2013 г.,* https://www.gartner.com/doc/id2510116
12. *Правила использования терминов: cybersecurity, cyber security, cybersecurity, Джо Франселла (Joe Franscella), Пер. Е. Бартов*
13. *Александр Федоров,* http://www.pircenter.org/media/content/files/10/13559195650.pdf
14. *Cyberspace Operations Concept Capability Plan 2016-2028*
15. *Доклад группы правительственных экспертов ООН, A/65/201*

Авторы:

Кузьмин Алексей
Доктор физико-математических наук, профессор, академик (Академия криптографии РФ)

Жуков Юрий
эксперт информационной безопасности

Финогенов Дмитрий
эксперт информационной безопасности

Информация взята из «BIS Journal» № 3(18)/2015 от 16 сентября, 2015