OSTIS-2015
(Open Semantic Technologies for Intelligent Systems)

УДК 004.432.4

ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ниязова Р.С., Буданова Н.

Евразийский национальный университет им. Л.Н.Гумилева,
г. Астана, Республика Казахстан

Rozamgul@list.ru
Emma9876@mail.ru

В работе описаны основные понятия информационной безопасности, онтологические задачи обеспечения информационной безопасности, классификации угроз информационной безопасности, модели реализации угроз информационной безопасности.
Ключевые слова: информационная безопасность; онтологические задачи; концептуальная модель; модель информационной безопастности.

Введение

Информация – это ценность. Утечка конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению и несанкционированному доступу к ее источникам.

В наше время безопасность информационных ресурсов может быть обеспечена только за счет комплекса системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др.

Мир находятся на пороге глобальных изменений: новое информационное общество приходит на смену обществу индустриальному, в связи с чем новые информационные технологии все более проникают в области деятельности человека, особенно в промышленность и общественную жизнь, ускоряя процессы глобализации и интеграции мировой экономики и мирового сообщества[8].

Таким образом, информационные системы являются одним из системообразующих факторов жизни современного общества, и влияние информационной безопасности и на все стороны жизни общества с течением времени будет только возрастать [9].

1. Основные составляющие информационной безопасности

Информационная безопасность – это защищенность информации и поддержка инфраструктуры от случайных или преднамеренных воздействий как естественного, так и искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Под информацией в области защиты понимаются сведения, раскрываемые через демаскирующие признаки объектов защиты или путем несанкционированного доступа к техническим средствам обработки информации. Информационная технология - система технических средств и способов обработки информации. Информационный ресурс – совокупность данных и программ, задействованных при обработке информации техническими средствами.

Субъект информационных отношений – физическое или юридическое лицо, обладающее определенным правом по отношению к информационному ресурсу. В зависимости от уровня полномочий субъект информационных отношений может быть источником, собственником, владельцем или пользователем информации. Источник информации - материальный объект или субъект, способный накапливать, хранить, преобразовывать и выдавать информацию в виде сообщений или сигналов различной физической природы. Защита информации – комплекс

мероприятий, направленных на обеспечение информационной безопасности. Верный подход к проблемам информационной безопасности начинается с поиска субъектов информационных отношений и исследования интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – защита от несанкционированного доступа к информации.

При построении системы информационной безопасности предприятия предлагается модель (рисунок 1), которая описывает совокупность объективных внешних и внутренних факторов и демонстрирует их влияние на состояние информационной безопасности на объекте. Данная модель включает следующие объективные факторы: угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации; уязвимости информационной системы или системы контрмер, влияющие на вероятность реализации угрозы; риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности – утечки информации и ее неправомерного использования.

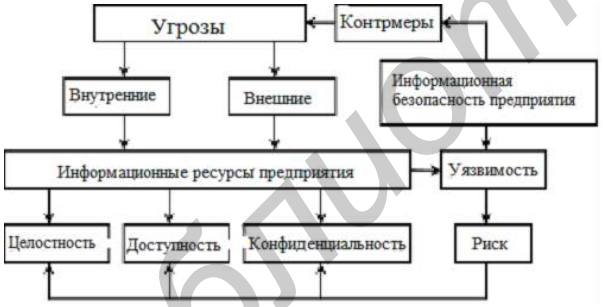

Рисунок 1 – Концептуальная модель информационной безопасности

Благодаря многоступенчатой структуре концептуальной модели информационной безопасности предприятия, введения системы контроля и закрепления ответственности, существенно снижается риск утечек конфиденциальной информации по вине человеческого фактора.

2. Онтология задачи обеспечения информационной безопасности

Опираясь на введенные выше понятия, можно построить следующую онтологическую схему задачи обеспечения информационной безопасности (рисунок 2)

Субъекты информационных отношений (источник, собственник, владелец или пользователь информации) определяют множество информационных ресурсов, которые должны быть защищены от различного рода атак. К активам

ИС обычно относят:

– материальные ресурсы;
– информационные ресурсы (аналитическая, служебная, управляющая информация на всех этапах своего жизненного цикла: создание, обработка, хранение, передача, уничтожение);
– информационные технологические процессы жизненного цикла автоматизированных систем;
– предоставляемые информационные услуги и т.п.[9].

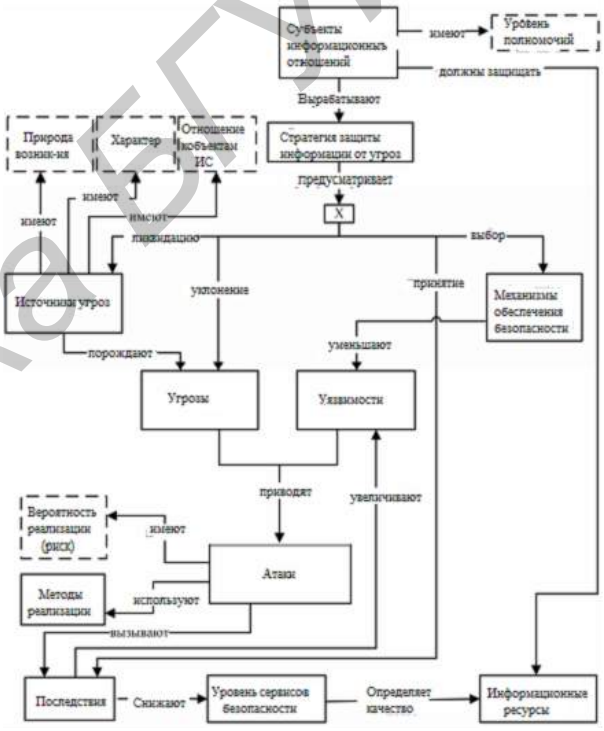

Рисунок 2 – Онтология задачи обеспечения безопасности информационных систем

Исходя их данного принципа, моделирование и классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки:

Источник угрозы – Угроза – Уязвимость – Реализация угрозы (атака) – Последствия (ущерб).

При этом под термином угроза понимается возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и/или потери информации.

3. Классификация угроз информационной безопасности

Обеспечение защиты информации невозможно без проведения системного анализа соответствующих угроз безопасности. Основу такого анализа должна составлять классификация угроз по определенным базовым признакам, дающая исследователю целостное представление о различных вариантах деструктивных воздействий и их последствиях.

Данные элементы при разработке классификации могут быть выбраны в качестве базовых классификационных признаков для последующей их декомпозиции.

Согласно ГОСТ Р 51275-2006 факторы, влияющие на информационную безопасность, можно подразделить по признаку отношения к природе их возникновения на объективные и субъективные, по отношению к объектам информационной системы - на внутренние и внешние.

Кроме этого, и внешние и внутренние источники могут носить как преднамеренный, так и непреднамеренный характер.

Непреднамеренные угрозы возникают независимо от воли и желания людей. Данный тип угроз связан чаще всего с прямым природным или техногенным физическим воздействием на элементы информационной системы и ведет к нарушению работы этой системы и/или физическому повреждению (уничтожению) носителей информации, средств обработки и передачи данных, телекоммуникационных каналов.

Причиной возникновения угроз непреднамеренного характера могут быть как сбои вследствие конкретных ошибок персонала и прямых действий иных лиц, так и случайные нарушения в работе системы.

Преднамеренные угрозы, в отличие от непреднамеренных, могут быть созданы только людьми, действующими целенаправленно с целью дезорганизовать работу информационной системы. Преднамеренные угрозы, в свою очередь, подразделяются на пассивные и активные.

Пассивные угрозы связаны с несанкционированным доступом к информации без каких-либо ее изменений. Активные угрозы связаны с попытками изменения информации или попытками лишения доступа к информационным ресурсам легитимных пользователей.

Общая схема классификации угроз информационной безопасности показана на рис.3

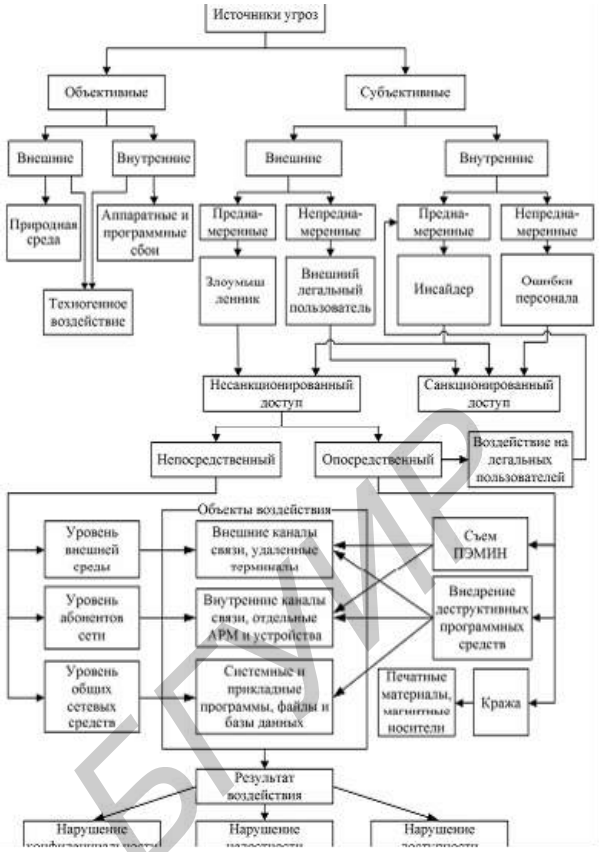

Рисунок 3 – Классификация угроз информационным ресурсам

Заключение

В современном мире уже не осталось сфер деятельности без применения компьютера и информационных систем. Человечество совершило большой рывок в области новых технологий. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. С каждым днем увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам. Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

Библиографический список

[**Шарипбаев А. А, Баймуратова Г. Г., 2005**] Шарипбаев А.А, Баймуратова Г.Г О требованиях к стандартизации программных средств, 2005г.

[**Попов В. Б., 2005**] Попов В.Б., Основы информационных и телекоммуникационных технологий. Основы информационной безопасности, 2005г.

[**Грушо А. А., Тимонина Е. Е., 1996**] Грушо А.А., Тимонина Е. Е., 1996 Теоретические основы защиты информации, 1996г.

[**Малюк А. А., 2004**] Информационная безопасность - концептуальные и методологические основы защиты информации, 2004г.

[**Бармен С., 2002**] Бармен С. Разработка правил информационной безопасности, 2002г.

[**Степанов Е. А., Корнеев И. К., 2001**] Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации, 2001г.

[**Барсуков В. С., 2001**] Барсуков В. С. Безопасность - технологии, средства, услуги., 2001г.

[**Кастельс М., 2000**] Информационная эпоха: экономика, общество и культура / Пер.с англ. под научи. ред. О. И. Шкаратана. М., 2000.

[**Ажмухамедов И. М., 2011**] Принципы обеспечения комплексной безопасности информационных систем // Вестник АГТУ. Серия: "Управление, вычислительная техника и информатика" №1/2011, С.7-11.

[**Ажмухамедов И. М., 2012**] Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования, 2011

ONTOLOGIC MODEL OF PROCESS OF ENSURING INFORMATION SECURITY

Niyazova R.S., Budanova N.

L.N. Gumilyov Eurasian University, Astana, Republic of Kazakhstan

Rozamgul@list.ru

Emma9876@mail.ru

Introduction

Information – this value. Leaks of confidential information bring moral or material damage. Conditions conducive to the mastery of inappropriate confidential information, reduced to its disclosure or unauthorized access to its source.

Main Part

In our time, the security of information resources can only be achieved through a complex system of information protection. Integrated security system should be: continuous, planned, focused, specific, active, reliable, and others. Methods of information security should be directed to the precise nature of actions directed to early action to prevent possible threats to commercial secrets.

Conclusion

Providing information security is achieved organizational, logistical and technical measures, each of which provides specific powers, means and measures with relevant characteristics.