Раздел 2. Экономика строительства

УДК 004.056.53 DOI 10.37279/2519-4453-2021-3-33-39

МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бойченко О.В.[1], Иванюта Д.В.[2]

[1] Институт экономики и управления (структурное подразделение), ФГАОУ ВО КФУ им. В.И. Вернадского, 295015, г. Симферополь, ул. Севастопольская, 21/4, e-mail: bolek61@mail.ru
[2] Институт экономики и управления (структурное подразделение), ФГАОУ ВО КФУ им. В.И. Вернадского, 295015, г. Симферополь, ул. Севастопольская, 21/4, e-mail: d.iwanyuta2011@yandex.ua

Аннотация. В данной статье рассмотрена проблема обеспечения информационной безопасности в современных условиях. Проведен анализ возможного решения данной проблемы с помощью построения моделей информационной безопасности: концептуальной, математической и функциональной. С учетом совершенствования стратегического управления информационной безопасностью и новых технологий в компьютерной сфере предпринята попытка детально рассмотреть концептуальную модель информационной безопасности, важность и необходимость которой связана с увеличением объемов передаваемых, используемых и хранимых данных, а также реализацией на практике защиты информационных прав пользователей с помощью предложенных механизмов.

Ключевые слова: модель, информационная безопасность, информация, концептуальная модель, математическая модель, функциональная модель, угрозы, защита информации.

ВВЕДЕНИЕ

В современном мире развитие информационных технологий достигло довольно высокого уровня, однако при этом возросло и количество преступлений в сфере компьютерной информации. Также появилась необходимость обеспечения эффективной защиты пользователей от несанкционированного вторжения и хищения информации. В связи с этим внимание специалистов информационной безопасности было акцентировано на исследовании компонентов безопасности и формировании моделей информационной безопасности. В данном направлении ведутся научные исследования, совершенствуются и разрабатываются планы защиты информации, которые могут обеспечить защиту каждого компонента от возможного негативного воздействия, способного вывести его из строя. Учитываются общие критерии безопасности информационных технологий и такие нарушения состояния их защищенности, как аварийные ситуации вследствие стихийных бедствий и отключения питания, отказы и сбои в работе аппаратуры, ошибки в программном обеспечении и работе сотрудников, помехи в линиях связи и возможные преднамеренные действия нарушителей.

Следовательно, при формировании модели информационной безопасности, требуется предусмотреть все механизмы для создания необходимого и достаточного уровня информационной безопасности, обеспечить противостояние угрозам и предусмотреть проведение эффективных мероприятий по ликвидации неблагоприятных последствий инцидентов информационной безопасности. Для сохранения достаточного уровня информационной безопасности рекомендуется применять построенные модели информационной безопасности в течение длительного времени.

АНАЛИЗ ПУБЛИКАЦИЙ, МАТЕРИАЛОВ И МЕТОДОВ

Словосочетание «информационная безопасность» рассматривают в разных контекстах, при этом оно может иметь различное толкование, а также использоваться в широком смысле. В Доктрине информационной безопасности РФ, утвержденной Указом Президента РФ от 5 декабря 2016 года №646 под информационной безопасностью Российской Федерации понимают «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[7].

Рассматривая это понятие в более узком смысле, мы предполагаем, что «информационная безопасность в современности основывается на концепции совокупной защиты данных, которая подразумевает применение определенного количества объединённых программно-аппаратных решений и мероприятий социального характера, поддерживающих и взаимодополняющих» [1,302 с.].

В направлении обеспечения безопасности информации особое внимание уделяют:

- соблюдению конфиденциальности, обеспечивая полный контроль доступа к информации, которую необходимо защитить, и одновременно сделать ее доступной для авторизированных пользователей, с учетом регулярного обновления паролей доступа;
- сохранению целостности информации, исключив несанкционированное изменение части информации третьими лицами, не имеющими к ней доступа;
- обеспечению доступности информации, то есть рассматриваются лица, которые имеют полный доступ к информации без каких- либо ограничений. В этом случае ответственность за сохранность возложена на допущенных к работе с данными.

Исторически сформировался подход к классификации информации с учетом уровня требований к сведениям с ограниченным доступом, обеспечения конфиденциальности информации. Этот факт можно объяснить тем, что ущерб, причиненный в результате разглашения открытой информации не будет настолько существенным. Например, для платежных документов важным является целостность и подлинность, а уже затем доступность, при этом требования к их конфиденциальности могут вообще не предъявляться. Поэтому важно также учитывать целостность, подлинность и доступность информации, которая не является конфиденциальной.

Также «для гарантирования информационной безопасности необходимо применение ряда мероприятий: выработать политику обеспечения защиты и составить соответствующую техдокументацию; внедрить технические средства обеспечения информационной безопасности» [3, С. 139-140].

Для обеспечения информационной безопасности создают модели безопасности, которые являются формальным (математическим, алгоритмическим, схематическим и т.п) выражением политики безопасности.

Учитывая непрерывность процесса данные модели должны постоянно совершенствоваться и обеспечивать на достаточном уровне устранение возможных слабостей, некорректностей и неисправностей.

ЦЕЛЬ И ПОСТАНОВКА ЗАДАЧИ ИССЛЕДОВАНИЯ

Целью данной работы является проведение анализа наиболее характерных источников образования угроз данным во взаимосвязи действий акторов социально-экономической системы региона для разработки и создания модели информационной безопасности в современных условиях развития рыночной экономики.

Учитывая нетривиальность процесса обеспечения информационной безопасности, понимая, что зачастую он требует немалых финансовых затрат, а в некоторых случаях является довольно дорогостоящим, мы поставили перед собой задачу детально рассмотреть основные модели обеспечения информационной безопасности, наиболее адекватных современным требованиям норм безопасности.

ОСНОВНОЙ РАЗДЕЛ

Вопрос обеспечения информационной безопасности информационных систем стоит одинаково остро перед обычными пользователями и перед предприятиями. Потеря данных влечет за собой потерю репутации и доверия, также сохраняется тенденция роста стоимости потерь при инцидентах.

Важность работы в данном направлении подтверждает инцидент, произошедший 2018 году, связанный с утечкой научных разработок в области ядерной физики, когда научные исследования из лучших британских университетов, включая Кембриджский университет, были украдены и перепроданы онлайн иранскими хакерами. Миллионы документов, включая секретные

исследования по атомным электростанциям и кибербезопасности стали товаром и были выставлены на продажу в Сети. Документ продавали как минимум за два фунта стерлингов (примерно 178 рублей). Хакеры также предлагали услуги по взлому баз данных британских университетов. «Глава отдела безопасности информации Эдинбургского университета подтвердил, что киберпреступники скачивали научные исследования. Были украдены пароли студентов и сотрудников университета, что вызвало необходимость в авральном режиме обновлять систему безопасности» [4].

Данный случай служит убедительным примером того, что обеспечение информационной безопасности должно предоставлять возможность выявления угроз безопасности с целью их блокирования и предотвращения неприемлемых негативных последствий в дальнейшем. Четко и своевременно поставленные задачи должны принимать во внимание риск принятия ошибочного или неоптимального решения. Решение данных вопросов направлено на координацию деятельности в области информационной безопасности и совершенствование создаваемых моделей информационной безопасности, что подчеркивает важность и актуальность исследования в данном направлении.

Построение системы информационной безопасности предполагает в обязательном порядке рассмотрение следующих объективных факторов:

-угроз информационной безопасности, вероятность их возникновения и реализации;

-уязвимостей системы информационной безопасности;

-риск и возможный ущерб в случае успешной реализации угрозы информационной безопасности, который найдет отражение в вероятных финансовых потерях – прямых или косвенных.

При создании модели информационной безопасности рассматривают такие защищаемые объекты, как объекты информатизации, ресурсы информационной системы, информационные системы, информационные технологии, программные средства, сети связи, автоматизированные системы. «Под объектом защиты понимается информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации» [6].

К объектам защиты также можно отнести охраняемую территорию, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Модели безопасности посредством системотехнического подхода, дают возможность рассмотреть решение следующих задач:

- выбор, обоснование базовых принципов архитектуры автоматизированных систем;
- подтверждение свойства защищенности системы;
- составления формальной спецификации политики безопасности разрабатываемых систем.

Последним важным вопросом при построении моделей или систем является их жизненный цикл, который включает следующие этапы:

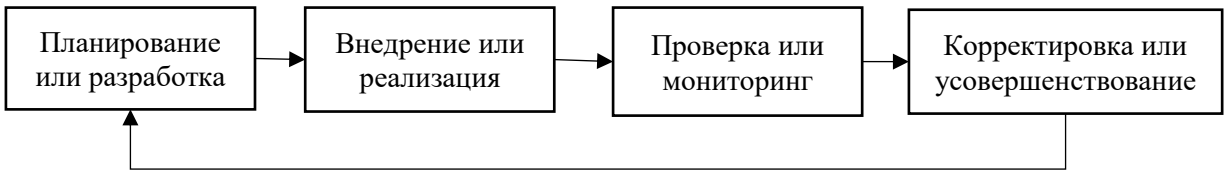

Рис. 1. Жизненный цикл системы информационной безопасности
Составлено авторами по материалам [8]

К основным моделям информационной безопасности относятся концептуальная, математическая и функциональная модели.

Концептуальная модель представляет собой множество понятий и связей между ними, которые определяют смысловую структуру исследуемой предметной области. Данная модель должна включать перечень взаимосвязанных понятий, включая их свойства, характеристики, классификацию, учитывая также типы, ситуации, признаки в данной области и условия протекания процесса. В этом случае правомерно рассмотреть возможные угрозы безопасности, источники возникновения рассматриваемых угроз, способы реализации, цели и другие условия, которые способны нарушить безопасность. Перечисленные компоненты определяют концептуальную

модель информационной безопасности, которая также включает объекты угроз, способы доступа, направления защиты, средства защиты, а также источники информации.

Таким образом, создание концептуальной модели информационной безопасности направлено на предоставление ответов на общие вопросы, схематически отражая при этом общую структуру модели, на основе которой будут строиться другие модели и концепции информационной безопасности. При этом, реализация концептуальной модели информационной безопасности рассматривает создание нескольких уровней. В основном – это сервисный и организационно-управленческий уровень.

Полная концептуальная модель информационной безопасности, которая является общей для всех информационных систем, представлена на рис. 2.

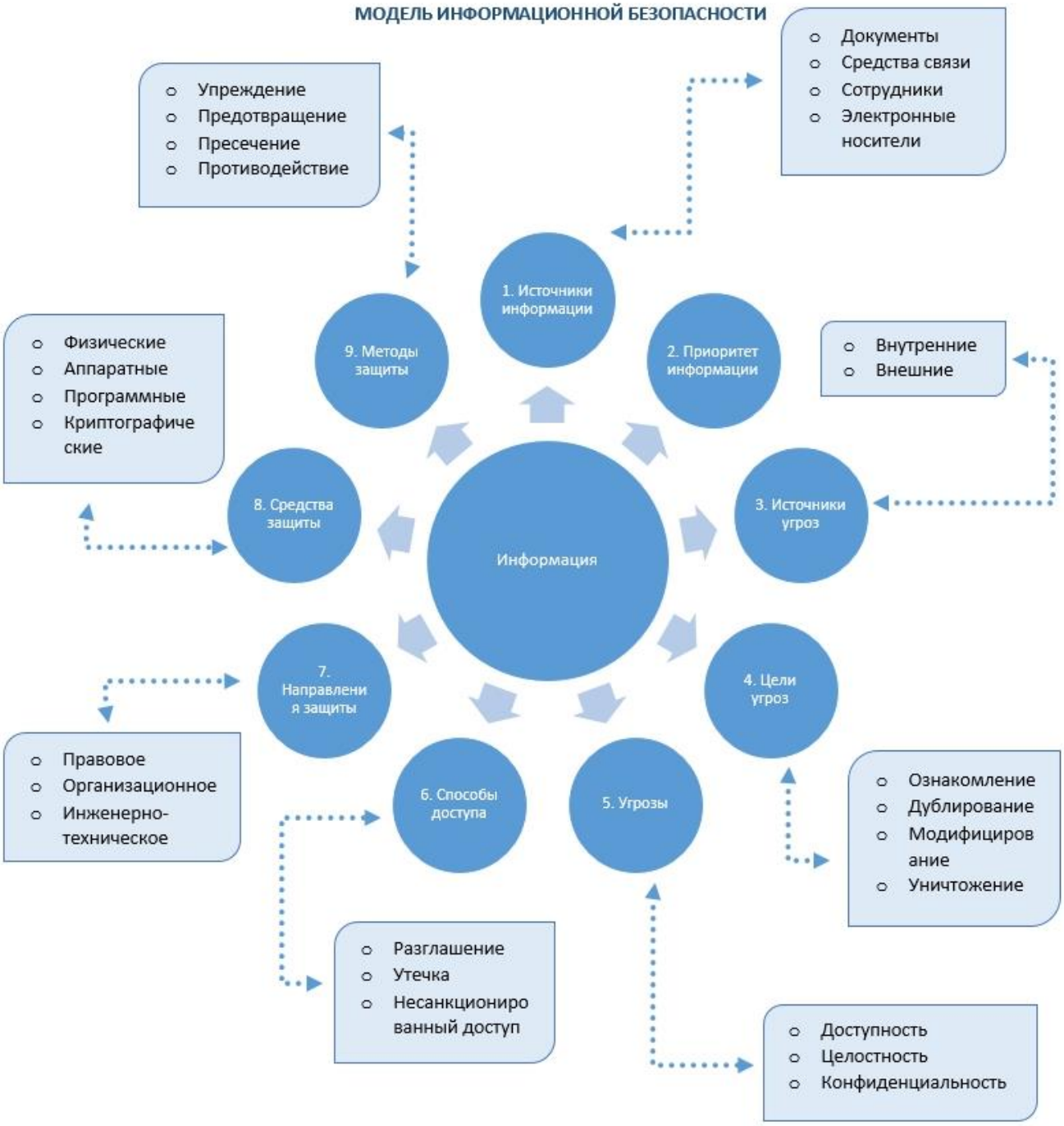

Рис. 2. Концептуальная модель ИБ
Составлено авторами по материалам [8]

Концептуальная модель безопасности информации определяет процесс разработки методических рекомендаций по ее внедрению, которые должны использоваться с учетом рассмотренных принципов и являться основой защиты информации.

После разработки концептуальной модели переходят к выстраиванию математической и функциональной модели информационной безопасности. Данные модели имеют неразрывные связи.

«Математическая модель в информационной безопасности — это описание сценариев в виде последовательности действий нарушителей и соответствующих ответных мер. Такие модели описывают процессы взаимодействия нарушителя с системой защиты и возможные результаты действий» [5, 93с.].

В процессе создания математической модели информационной безопасности проводится экспертная оценка вероятности киберугроз с учетом их значимости и степени финансовых трат на восстановление нормального функционирования системы и сохранения данных после кибератак и утечек информации. Также производят расчет общего риска отказа системы.

Необходимость таких расчетов имеет очень большое значение для экономики России. К примеру, уже проанализирован ущерб российской экономики к началу 2022 года, который может составить до 6 трлн. Рублей. Такие крупные потери могут быть вызваны атакой шифровальщика, который заблокирует поставки нефти или газа, чем вызовет огромные экономические потери. Вирусом-шифровальщиком можно обесточить больницу. При этом, люди, которые будут в реанимации окажутся под угрозой смерти. При этом невозможно оценить человеческую жизнь в подобной ситуации.

Таким образом, математическая модель информационной безопасности позволяет [2, 9]:

-оценить возможность реализации различных угроз на информационные системы и проведения атак на них;

– дать количественную оценку качества функционирования системы защиты;

– оценить экономическую эффективность применения средств защиты информации;

— определить структуру построения системы защиты информационной системы.

Если в итоге общие денежные траты на устранение рисков меньше или равны максимальному уровню затрат, которые выделяются на снижение или устранение суммарных рисков, систему информационной безопасности считают финансово оправданной.

В дальнейшем на базе сформированной математической модели создается функциональная модель, которая в свою очередь требует особого внимания, учитывая рассмотрение конкретных мер по защите. Функциональная модель определяет функции служб защиты информации, которые должны быть реализованы. При этом, требуется предоставить упорядоченный набор функций, с учетом входных данных (материальных объектов), ограничений, исполнителей, ожидаемого результата.

Отдельно хотелось бы уделить внимание преступлениям в сфере информационной безопасности, которые могут осуществляться через человека. К ним относятся хищение носителей информации, ознакомление с информацией без разрешения владельца. С помощью программ можно осуществлять преступления путем перехвата паролей, копирования информации с носителей, дешифровки. Хищение информации возможно с помощью подключения специальных аппаратных средств доступа к информации, а также посредством перехвата побочных электромагнитных излучений от аппаратуры. Кроме того, информационная безопасность персональных данных может подвергаться атаке со стороны компьютерных сетей и распространения известных видов троянских программ. Также нельзя забывать, что средства нападения, способные обмануть защиту информации, постоянно развиваются и совершенствуются.

К примеру, криптосистема DES, являющаяся стандартом шифрования в США с 1977 г., на сегодняшний день может быть раскрыта методом «грубой силы» - прямым перебором.

Подобные случаи в международной практике также требуют изучения и анализа, так как в процессе формирования моделей информационной безопасности нужно учитывать лучшие идеи зарубежных организаций и современные требования к работе над созданием тех или иных моделей.

ВЫВОДЫ

Следовательно, модели информационной безопасности обеспечивают формализацию политик безопасности и определяют единый подход с учетом ключевых особенностей объектов и ожидаемых результатов в процессе применения той или иной модели. Предоставленный набор правил дает возможность проецирования абстрактных положений в политику безопасности, которая будет применяться при проектировании программного и аппаратного обеспечения. При этом, в основе системы защиты информации должна быть концептуальная модель информационной безопасности.

В заключении хочется подчеркнуть, что защита информации не ограничивается техническими методами. Проблема значительно шире. К недостаткам защиты можно отнести и людей, а также их отношение к обеспечению надежности системы безопасности.

Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ

Прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий стал решающим условием создания современных средств обеспечения безопасности, что требует во многом предусмотреть научную парадигму информационной безопасности. На сегодняшний день теория информационной безопасности – одна из самых развивающихся естественных наук.

Заинтересованность российских компаний, учреждений и предприятий в использовании моделей информационной безопасности, несомненно, есть. Это уже действительность. В дальнейшем популярность таких моделей будет неуклонно расти, учитывая экономическую целесообразность.

Очевидно, что мы имеем дело с важным направлением совершенствования информационной системы, которое выражается в изучении существующих проблем и определении всех возможных злоумышленных действий по отношению к системе, требует постоянного совершенствования и проведения глубокого анализа с целью создания моделей информационной безопасности. Качественное построение модели требует агрегировать знания и совмещать подходы, полученные из разных источников, адаптации к конкретным условиям, учитывать современные отечественные и зарубежные стандарты.

Развитию теории информационной безопасности особое внимание уделяют центры компьютерной безопасности. В России такими центрами являются Государственная техническая комиссия при Президенте Российской Федерации, Институт криптографии, связи и информатики Академии ФСБ, Академия криптографии Российской Федерации.

ЛИТЕРАТУРА

1. Апатова, Н.В. Информационная безопасность социально-экономических систем: монография [Текст] / Апатова Н.В, Акинина Л.Н., Байздренко Е.А., Бойченко О.В., Гапонов А.И., Герасимова С.В., КоролевО.Л., Писарюк С.Н., Потанина М.В., Рыбников А.М., Рыбников М.С., Ремесник Е.С., Смирнова О.Ю., Титаренко Д.В. и др. / под ред. Проф. О.В Бойченко. – Симферополь: ИП Зуева Т.В., 2017 – 302 с.

2. Артем, П. Модель информационной безопасности [Текст] / П. Артем // CISO CLUB Информационная безопасность октябрь 2020. [Электронный ресурс] – Режим доступа: https://cisoclub.ru/model-informaczionnoj-bezopasnosti/# (дата обращения: 18.07.2021).

3. Бойченко О.В. Система комплексной защиты данных в корпоративных сетях [Текст] / О.В. Бойченко, А.С. Ивченко // Проблемы информационной безопасности: IV Междунар. Науч.-технич. Конф., 15-17 февраля 2018 г.: тезисы докладов. – Симферополь- Гурзуф, 2018 – С.139-140.

4. Кубарев, А. Иранские хакеры перепродавали исследования престижных вузов Англии [Текст] / А. Кубарев. Сентябрь 2018. [Электронный ресурс] – Режим доступа: URL: https://polit.info/420847-iranskie-khakery-pereprodavali-issledovaniya-prestizhnykh-vuzov-anglii (дата обращения: 10.07.2021).

5. Щеглов, А.Ю. Математические модели и методы формального проектирования системы защиты информационных систем [Текст] / А.Ю. Щеглов, К.А. Щеглов: учеб. Пособие. СПб.: Университет ИТМО, 2015, 93с.

6. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. Взамен ГОСТ Р 50922-96. Введ. 2008-02-01 // СПС «Кон-сультантПлюс»

7. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] – Режим доступа: URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 16.07.2021).

8. Itnan. Модели информационной безопасности. 2020 г.м [Электронный ресурс] – Режим доступа: URL: https://itnan.ru/post.php?c=1&p=347088 (дата обращения: 14.07.2021).

9. Ветрова, Н.М. Особенности менеджмента информационной безопасности на современном этапе [Текст] / Н.М. Ветрова, А.А. Гайсарова //Экономика строительства и природопользования. – 2017. – № 1(62). – С. 64–70

INFORMATION SECURITY MODELS

Boychenko O.V.[1], Ivanyuta D.V.[2]

[1,2] Institute of Economics and Management, V. I. Vernadsky Crimean Federal University, Simferopol, Crimea

Annotation. This article considers the problem of ensuring information security in modern conditions. The analysis of a possible solution to this problem is carried out by constructing information security models: conceptual, mathematical and functional. Taking into account the improvement of strategic information security management and new technologies in the computer sphere, an attempt is made to consider in detail the conceptual model of information security, the importance and necessity of which is associated with an increase in the volume of transmitted, used and stored data, as well as the implementation in practice of protecting the information rights of users using the proposed mechanisms.

Keywords: model, information security, information, conceptual model, mathematical model, functional model, threats, information protection.