ПРОБЛЕМЫ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Руденя В.Ю.

Магистрант кафедры проектирования информационно-компьютерных систем, Белорусский государственный университет информатики и радиоэлектроники (БГУИР), г.Минск

Аннотация

Статья посвящена проблеме защиты данных в информационных системах, описываются основные требования и свойства для защиты информационных сетей и систем.

Ключевые слова: Подходы и принципы, обеспечение безопасности, технологическая безопасность, информационные системы.

Под обеспечением безопасности информационных систем понимают меры, предохраняющие информационную систему от случайного или преднамеренного вмешательства в режимы ее функционирования.

Существует два принципиальных подхода к обеспечению компьютерной безопасности для предприятий [1]:

1. Фрагментарный. Данный подход ориентируется на противодействие строго определенным угрозам при определенных условиях (например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д.).

Достоинством фрагментарного подхода является его высокая избирательность относительно конкретной угрозы. Недостатком – локальность действия, т.е. фрагментарные меры защиты обеспечивают эффективную защиту конкретных объектов от конкретной угрозы. Но не более того [2].

2. Комплексный. Данный подход получил широкое распространение вследствие недостатков, присущих фрагментарному. Он объединяет разнородные меры противодействия угрозам и традиционно рассматривается в виде трех дополняющих друг друга направлений. Организация защищенной среды обработки информации позволяет в рамках существующей политики безопасности обеспечить соответствующий уровень безопасности АИС. Недостатком данного подхода является высокая чувствительность к ошибкам установки и настройки средств защиты, сложность управления [3].

Особенностью комплексного подхода к защите информации является создание защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические. Организация подобной защищенной среды позволяет гарантировать определенный уровень безопасности автоматизированной информационной системы [4].

Комплексный подход к защите информации базируется на следующих методологических принципах [5]:

– конечной цели, абсолютного приоритета конечной (глобальной) цели;

– единства, совместного рассмотрения системы как целого и как совокупности частей (элементов);

– связности, рассмотрения любой части системы совместно с ее связями с окружением;

– модульного построения, выделения модулей в системе и рассмотрения как совокупности модулей;

– иерархии, введения иерархии частей (элементов) и их ранжирования;

– функциональности, совместного рассмотрения структуры и функции с приоритетом функции над структурой;

– развития, учета изменяемости системы, ее способности к развитию, расширению, замене частей, накапливанию информации;

– децентрализации, сочетания в принимаемых решениях и управлении централизации и децентрализации;

– неопределенности, учета неопределенностей и случайностей в системе.

В настоящий момент можно выделить следующие методологические, организационные и реализационные ***принципы информационной безопасности для предприятия*** [6]:

1. **Принцип законности.** Состоит в следовании действующему законодательству в области обеспечения информационной безопасности.
2. **Принцип неопределенности.** Возникает вследствие неясности поведения субъекта, т.е. кто, когда, где и каким образом может нарушить безопасность объекта защиты.
3. **Принцип невозможности создания идеальной системы защиты.** Следует из принципа неопределенности и ограниченности ресурсов указанных средств.
4. **Принципы минимального риска и минимального ущерба.** Вытекают из невозможности создания идеальной системы защиты. В соответствии с ним необходимо учитывать конкретные условия существования объекта защиты для любого момента времени.
5. **Принцип безопасного времени.** Предполагает учет абсолютного времени, т.е. в течение которого необходимо сохранение объектов защиты; и относительного времени, т.е. промежутка времени от момента выявления злоумышленных действий до достижения цели злоумышленником.
6. **Принцип «защиты всех ото всех».** Предполагает организацию защитных мероприятий против всех форм угроз объектам защиты, что является следствием принципа неопределенности.
7. **Принципы персональной ответственности.** Предполагает персональную ответственность каждого сотрудника предприятия, учреждения и

организации за соблюдение режима безопасности в рамках своих полномочий, функциональных обязанностей и действующих инструкций.

8. Принцип ограничения полномочий. Предполагает ограничение полномочий субъекта на ознакомление с информацией, к которой не требуется доступа для нормального выполнения им своих функциональных обязанностей, а также введение запрета доступа к объектам и зонам, пребывание в которых не требуется по роду деятельности.

9. Принцип взаимодействия и сотрудничества. Во внутреннем проявлении предполагает культивирование доверительных отношений между сотрудниками, отвечающими за безопасность (в том числе информационную), и персоналом. Во внешнем проявлении – налаживание сотрудничества со всеми заинтересованными организациями и лицами (например, правоохранительными органами).

10. Принцип комплексности и индивидуальности. Подразумевает невозможность обеспечения безопасности объекта защиты каким-либо одним мероприятием, а лишь совокупностью комплексных, взаимосвязанных и дублирующих друг друга мероприятий, реализуемых с индивидуальной привязкой к конкретным условиям.

11. Принцип последовательных рубежей безопасности. Предполагает как можно более раннее оповещение о состоявшемся посягательстве на безопасность того или иного объекта защиты или ином неблагоприятном происшествии с целью увеличения вероятности того, что заблаговременный сигнал тревоги средств защиты обеспечит сотрудникам, ответственным за безопасность, возможность вовремя определить причину тревоги и организовать эффективные мероприятия по противодействию.

12. Принципы равнопрочности и равномощности рубежей защиты. Равнопрочность подразумевает отсутствие незащищенных участков в рубежах защиты. Равномощность предполагает относительно одинаковую величину защищенности рубежей защиты в соответствии со степенью угроз объекту защиты.

Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий. Он означает оптимальное сочетание программных аппаратных средств и организационных мер защиты, подтвержденное практикой создания отечественных и зарубежных систем защиты [7].

Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки. Пользователям предоставляется минимум строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации.

Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ЭИС без ее предварительной регистрации [8].

СПИСОК ЛИТЕРАТУРЫ

1. Подходы, принципы, методы и средства обеспечения безопасности // Блог Святика [Электронный ресурс]. – 2018. – Режим доступа: https://svyatik.org/svarka-77790.html. – Дата доступа: 05.04.2018.

2. Мамедова, К.А. Основные принципы обеспечения информационной безопасности страны / К.А. Мамедова. – М.: Информационная безопасность регионов №1 (22), 2016.

3. Обеспечение информационной безопасности организации // Международная торговая палата [Электронный ресурс]. – 2018. – Режим доступа: http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti. – Дата доступа: 15.04.2018.

4. Ясенев, В. Н. Информационная безопасность в экономических системах: Учебное пособие / В.Н. Ясенев. – Н. Новгород: Изд-во ННГУ, 2011.

5. Подходы, принципы, методы и средства обеспечения безопасности // Финлит.онлайн [Электронный ресурс]. – 2018. – Режим доступа: http://finlit.online/osnovyi-ekonomiki/podhodyi-printsipyi-metodyi-sredstva-4218.html. – Дата доступа: 22.04.2018.

6. Казарин, О.В. Безопасность программного обеспечения компьютерных систем / О.В. Казарин. – Москва: МГУЛ, 2013.

7. Жуков, В.Г. Модель нарушителя прав доступа в автоматизированной системе. / В.Г. Жуков, М.Н. Жукова, А.П. Стефаров. – Красноярск: СибГУ 2012.

8. Комплексный подход к организации системы защиты информации на предприятии: основные вопросы и технологии // ЕПАМ [Электронный ресурс]. – 2018. – Режим доступа: https://www.epam-group.ru/about/news-and-events/in-the-news/2009/kompleksnyy-podhod-k-organizacii-sistemy-zaschity-informacii-na-predpriyatii-osnovnye-voprosy-i-tehnologii. – Дата доступа: 23.04.2018.