Сиротюк В.О., Грузман В.А., Косяченко С.А.

Структура и характеристики объектов информационной безопасности и классификация информационных ресурсов

Аннотация: В работе рассмотрена классификация объектов информационной безопасности организаций. Описаны их структура и характеристики. Предложена методика классификации информационных ресурсов для определения уровня защиты информации от несанкционированного доступа. Предложенные подходы и методы позволяют уменьшить трудоемкость разработки и внедрения системы информационной безопасности организаций, повысить эффективность ее функционирования.

Ключевые слова: информационная безопасность, объект информационной безопасности, информационные ресурсы, информационная инфраструктура, обеспечивающая инфраструктура, открытая информация, конфиденциальная информация, служебная информация

Введение

В условиях глобализации бизнеса, перевода экономики на цифровую платформу предприятия и организации с каждым годом расширяют свое информационное представительство как в отдельном регионе, стране, так и в мировом информационном пространстве, наращивают свой информационный потенциал, совершенствуют автоматизированные информационно-управляющие и поисковые системы, расширяют электронное взаимодействие с внешними организациями. Вместе с этим возрастают потенциальные угрозы и риски их информационной безопасности и, как следствие этого, возрастает потребность в надежных и эффективных методах и средствах защиты данных, информационной и обеспечивающей инфраструктуры, обеспечения их сохранности и восстановления в случае сбоев, в основе которых должна лежать сбалансированная и эффективная система информационной безопасности [1].

Большую актуальность вопросы обеспечения информационной безопасности приобретают в современных условиях в связи с

возможностью, а также, зачастую, с необходимостью (например, в условиях пандемии коронавируса) организации работы сотрудников организации в дистанционном режиме. Предоставляя возможность удаленного доступа сотрудникам, находящимся вне защищаемого периметра, с помощью мобильных устройств (гаджетов) к информационным и сетевым ресурсам организации, резко увеличиваются риски информационной безопасности.

Для построения эффективной системы управления информационной безопасностью (СУИБ) на начальных этапах должны быть выполнены работы по выявлению, анализу, систематизации и классификации объектов информационной безопасности. Полученные результаты используются в дальнейшем для определения сферы (границ) СУИБ, разработки политики информационной безопасности организации, разработки механизмов и системы защиты данных, разработки планов восстановительных работ и др. работ по построению СУИБ [1,2].

В настоящей работе приведена классификация объектов информационной безопасности и описаны их характеристики, приведена методика классификации информации для определения уровня защиты информационных ресурсов.

Использование полученных в работе результатов позволяет повысить не только эффективность создания и функционирования СУИБ, но и уменьшить трудоемкость ее разработки и внедрения.

Объекты информационной безопасности и их характеристики

Основными объектами информационной безопасности (ИБ) организации являются:

- информационные ресурсы;
- информационная инфраструктура;
- обеспечивающая инфраструктура.

Рассмотрим характеристики объектов защиты.

Структура и характеристики информационных ресурсов подробно рассмотрены в следующем разделе настоящей статьи.

В данном разделе рассмотрим структуру и характеристики информационной и обеспечивающей инфраструктуры.

Информационную инфраструктуру можно разделить на 2 типа систем и средств: сетевая и телекоммуникационная инфраструктура

и автоматизированные информационно-управляющие системы и информационные технологии (АИУС и ИТ).

К первому типу относятся локальная сеть и сетевое оборудование ведомства, серверы, общесистемное программное обеспечение; каналы связи; интернет-коммуникации; компьютеры пользователей и прикладное программное обеспечение. Для обеспечения нормального функционирования сетевой и телекоммуникационной инфраструктуры необходимо приобретать сертифицированное оборудование, а также защищать входящее в ее состав оборудование от краж и повреждений. Для поддержания работоспособности целесообразно дублировать ответственные узлы, регулярно проводить регламентное обслуживание.

Ко второму типу относятся АИУС и ИТ, поддерживаемые и сопровождаемые в организации для обеспечения технологических процессов и производственной деятельности. Безопасность функционирования АИУС и ИТ во многом зависит от физического окружения, в котором они работают. Поэтому в процессе их эксплуатации необходимо постоянно поддерживать защиту системы, ее информационного обеспечения (баз данных), окружающей инфраструктуры и аппаратных средств.

К обеспечивающей инфраструктуре относятся системы электропитания, кондиционирования, водо- и теплоснабжения, пожарной сигнализации и др. Как показывает практический опыт, наибольшую проблему обеспечения безопасности обеспечивающей инфраструктуры представляют аварии водопроводной сети, пожары, перегрев серверных помещений (особенно в жаркое летнее время). В принципе к системам обеспечивающей инфраструктуры применимы те же требования по обеспечению ИБ, что и к различным видам обеспечений АИС.

Обеспечение безопасности информационных ресурсов и методы классификации информации

Для определения необходимого уровня защиты той или иной информации она должна быть классифицирована.

Разработанный алгоритм классификации информационных ресурсов включает следующие основные шаги (этапы):

1. Определение классов информации в соответствии с деятельностью организации.

2. Классификация обрабатываемой, хранимой и передаваемой в организации информации.

3. Составление перечня классифицированной информации и поддержание его в актуальном состоянии.

4. Маркирование информации.

Рассмотрим каждый из этапов классификации информации.

Информация делится на следующие классы: открытая информация, конфиденциальная информация, информация для внутреннего (служебного) использования.

К открытой информации относятся сведения, которые признаются общедоступными в соответствии с национальным законодательством, а также с принятой в организации политикой ИБ, и могут быть обнародованы. В частности, к ней относятся сведения, публикуемые в СМИ и на веб-сайте организации, информация рекламного характера, справочные, нормативные, правовые и методические документы и другая информация. К этой информации предъявляются требования по обеспечению полноты, достоверности, актуальности, доступности и сохранности данных, защиты ее от разрушений и модификации.

Доступ к конфиденциальной информации, ее обработка и хранение регламентируются соответствующими нормативными правовыми актами организации. К конфиденциальной информации относятся персональные данные служащих, данные бухгалтерской отчетности, отдельные виды управленческой информации, сведения об информационной инфраструктуре организации и другая информация. К этой информации предъявляются требования по обеспечению защиты ее от несанкционированного доступа, а также по обеспечению достоверности и сохранности данных.

Обработка конфиденциальной информации допускается только с применением сертифицированных программно-аппаратных средств. Методы и средства передачи конфиденциальной информации должны обеспечивать ее передачу только адресатам с обязательной идентификацией и подтверждением авторства отправителя и факта получения. При передаче конфиденциальной информации в цифровой форме обязательно ее шифрование. Хранение конфиденциальной информации должно осуществляться с использованием средств контроля актуальности и достоверности

данных. Процессы уничтожения конфиденциальной информации должны обеспечивать невозможность ее восстановления.

К информации для внутреннего использования относятся внутренние организационно-распорядительные документы, нормативно-справочная информация, внешняя и внутренняя служебная переписка, проекты договоров и прочая информация, которая не отнесена к открытой и конфиденциальной.

Доступ лиц к информации данного класса при ее обработке, хранении, передаче и уничтожении должен осуществляться на основании трудовых соглашений или договорных отношений, в объемах, минимально необходимых для исполнения своих должностных обязанностей допущенным лицом.

Классификация обрабатываемой, хранимой и передаваемой в ведомстве информации проводится на основе ее инвентаризации и предполагает составление и последующее ведение (поддержание в актуальном состоянии) перечней открытой и конфиденциальной информации, а также информации для внутреннего (служебного) использования. Классификацию информационных ресурсов осуществляет подразделение, ответственное за информационную безопасность организации, путем присвоения каждому виду информации определенного класса: открытая информация, для внутреннего использования, конфиденциальная.

При этом перечень конфиденциальной информации должен утверждаться руководством организации и доводиться до всех руководителей структурных подразделений организации.

В соответствии с принятой схемой классификации информации в дальнейшем производится ее маркирование. При этом на документы или другие материальные носители информации, содержащие сведения, отнесенные к конфиденциальной информации, проставляется гриф конфиденциальности.

Заключение

В работе рассмотрены методы и методики классификации объектов информационной безопасности. Особое внимание уделено методам классификации информационных ресурсов для определения уровня их безопасности и защиты. Полученные результаты используются в дальнейшем при построении оптимальной системы управления информационной безопасностью.

Предложенные подходы и методы использовались при построении системы информационной безопасности международной региональной патентной организации – Евразийского патентного ведомства Евразийской патентной организации [3].

Данная работа подготовлена в рамках программы Президиума РАН № 30 (7) «Теория и технологии многоуровневого децентрализованного группового управления в условиях конфликта и кооперации»

Литература:

1. *Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О.* Теоретические основы проектирования оптимальных структур распределенных баз данных. Серия «Информатизации России на пороге XXI века». – М.: СИНТЕГ, 1999. – 660 с.

2. *Кульба В.В., Сиротюк В.О.* Формализованная методология повышения эффективности и качества патентных информационных фондов и опыт ее использования при формировании и развитии евразийского патентно-информационного пространства. – М.: ИПУ РАН, 2019. – 236 с.

3. *Кульба В.В., Сиротюк В.О., Косяченко С.А.* Информационная безопасность патентных ведомств: теория и практика. – М.: ИПУ РАН, 2017. – 166 с.

Анохин А.М.

Организация компактной визуализации информационных параметров в системах контроля и управления

Аннотация: Реализация интерактивных систем контроля и управления связана с представлением большого объема быстроменяющихся параметров. При этом необходимо обеспечить возможность адекватного восприятия человеком-оператором представленной информации для принятия осознанных и эффективных управляющих действий. Предлагаются конкретные решения проблемы. Приводится пример использования этих решений.

Ключевые слова: интерактивный режим, человек-оператор, информационные параметры, визуализация