УДК 004.056.5

ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ. ВОПРОСЫ БЕЗОПАСНОСТИ

Кечкина Н.И., Наумова Е.Г.

Дзержинский политехнический институт (филиал)
ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева»,
Дзержинск, e-mail: nataliyabaranova@yandex.ru, soboll007@yandex.ru

В статье рассматриваются вопросы безопасности информации в информационных системах органов государственного и муниципального управления. Для достижения поставленной цели решен ряд задач. Для начала рассмотрено понятие информационных систем и представлена их классификация. Особое внимание уделяется группе государственных информационных систем. Поскольку данные системы предполагают обращение большого объема разнородной информации, то вопросы информационной безопасности в данной области являются наиболее актуальными и требуют неотложного решения. Основная цель работы – рассмотреть вопросы безопасности государственных информационных систем, обозначить возможные способы защиты информации. Для достижения поставленной цели проведен анализ информации, циркулирующей в государственных информационных системах. Предлагается классифицировать информацию на общедоступную и информацию с ограниченным доступом. Направления и класс защиты выбирают исходя из уровня значимости информации, а также размера информационной системы. Представлена классификация возможных угроз. Основной принята классификация по аспектам, на которые угрозы направлены: угрозы доступности, угрозы целостности и угрозы конфиденциальности. Для каждого типа приведена характеристика угроз и предложены мероприятия и средства по обеспечению информационной безопасности. Отмечается, что для обеспечения требуемого уровня информационной безопасности стоит рассматривать совокупность организационно-правовых и программно-технических средств.

Ключевые слова: государственные информационные системы, класс защиты, уровень значимости информации, масштабы информационной системы, угрозы безопасности информации

STATE INFORMATION SYSTEMS. SECURITY QUESTIONS

Kechkina N.I., Naumova E.G.

Dzerzhinsk Polytechnic Institute, R.E. Alekseev Nizhny Novgorod State Technical University,
Dzerzhinsk, e-mail: nataliyabaranova@yandex.ru, soboll007@yandex.ru

The article deals with the issues of information security in information systems of state and municipal authorities. To achieve this goal, a number of tasks have been solved. To begin with, the concept of information systems is considered and their classification is presented. Particular attention is paid to the group of state information systems. Since these systems involve the circulation of a large amount of heterogeneous information, the issues of information security in this area are the most urgent and require an urgent solution. The main purpose of the work is to consider the security issues of state information systems, to outline possible ways to protect information. To achieve this goal, the analysis of information circulating in state information systems was carried out. It is proposed to classify information into public and restricted information. The level of significance of information and the scale of the information system make it possible to determine the class of protection, and therefore to choose the direction of protection. The classification of possible threats is presented. The main classification is adopted according to the aspects to which the threats are directed: threats to availability, threats to integrity and threats to confidentiality. For each type, the characteristics of threats are given and measures and means for ensuring information security are proposed. It is noted that to ensure the required level of information security, it is worth considering a set of organizational and legal and software and hardware tools.

Keywords: state information systems, protection class, information significance level, information system scale, information security threats

В соответствии с ГОСТ Р 52653-2006 информационные технологии (ИТ) представляют собой совокупность методов и способов сбора, передачи, накопления, обработки, хранения, представления и использования информации.

В настоящее время обязательным элементом компьютерной ИТ является наличие вычислительной техники, а также телекоммуникационных средств, интуитивно-понятного пользовательского интерфейса.

Структура компьютерной ИТ включает:

– технические средства, в том числе средства вычислительной, коммуникационной и организационной техники;

– программные средства: системное (общее) и прикладное программное обеспечение;

– инструкции, нормативные документы, методические материалы по организации работы, образующие организационно-методическое обеспечение [1].

Информационная система (ИС) является средой реализации информационной технологии. ИС организации предполагает наличие и взаимосвязь средств накопления, обработки, передачи, хранения и контроля информации, формирующие информационную инфраструктуру, а также персонала, выполняющего эти действия с информацией.

Согласно определению, приведенному в ГОСТ Р 52653-2006, информационная система – это совокупность содержащейся в базах данных информации, а также обеспечивающих ее обработку информационных технологий и технических средств.

Среди многочисленных целей функционирования ИС организации основной является производство информации, необходимой для функционирования организации. Для поддержания возможности управления ИС организацией необходимой является реализация информационной и технической сред. ИТ позволяют осуществить в ИС все необходимые процессы преобразования информации.

Цель исследования – выявить основные угрозы информационной безопасности и на основе их анализа определить средства, необходимые для формирования системы информационной безопасности государственных информационных систем (ГИС).

Материалы и методы исследования

С использованием методов анализа и синтеза в исследовании проводится выявление основных направлений и методов обеспечения информационной безопасности. На основе современных публикаций, законов РФ в области информационных технологий и систем, методических документов, отражающих меры защиты информации в государственных информационных системах, рассмотрена классификация информационных систем, способы оценки класса защиты, определены направления защиты.

Результаты исследования и их обсуждение

Далее (рисунок) приводится классификация ИС, сформированная в соответствии с ч. 1 ст. 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ [1].

Если коснуться более подробно государственных и муниципальных ИС, то первые создаются на основании федеральных законов, законов субъектов Российской Федерации, а также на основании правовых актов государственных органов [2].

Муниципальные ИС разрабатываются на основании решения органа местного самоуправления [2].

И государственные, и муниципальные ИС необходимы для организации обмена информацией между органами государственного и муниципального управления (ГМУ), между органами управления и юридическими и физическими лицами, а также в информировании общества [2].

При рассмотрении информационных систем с точки зрения безопасности выделяют субъекты (активные компоненты) и объекты (пассивные компоненты).

К субъектам государственных ИС относят госслужащих, обслуживающий ИС персонал, представителей юридических лиц и физических лиц, которые могут обращаться к ИС по различным вопросам.

Объектами ИС являются информация и информационные процессы. В информационных системах ГМУ циркулирует самая разная информация, в первом приближении она делится на общедоступную информацию и информацию ограниченного доступа.

К категории общедоступной информации относят как общеизвестные сведения, так и иные данные, доступ к которым не должен быть ограничен. Это позволяет использовать и размещать ее свободно любыми лицами, в том числе в сети Интернет в открытом доступе, если это не противоречит установленным федеральными законами ограничениям в отношении распространения подобной информации. Так, для государственных ИС согласно ст. 13 Федерального закона от 09.02.2009 № 8-ФЗ в сети Интернет может быть размещена общая информация о деятельности государственных органов и органов местного самоуправления [3]. В ст. 14 этого же закона дополнительно указан состав общедоступной информации, размещаемой в сети «Интернет», в том числе в форме открытых данных [3].

Классификация ИС

Разновидности ИС ГМУ РФ в зависимости от масштаба

Масштаб	Область функционирования	Сегменты
ИС федерального масштаба	В пределах федерального округа РФ [5]	Сегменты находятся в субъектах РФ, муниципальных образованиях и организациях [5]
ИС регионального масштаба	На территории отдельного субъекта РФ [5]	Сегменты находятся в одном или нескольких муниципальных образованиях и подведомственных и других организациях [5]
ИС объектового масштаба	На территории одного федерального органа государственной власти (ОГВ), ОГВ субъекта РФ, муниципального образования и организации [5]	Не имеют сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях [5]

Информацией ограниченного доступа являются государственная тайна и конфиденциальная информация. Последняя в свою очередь разбивается на следующие типы: коммерческая тайна, персональные данные, служебная информация и т.п.

Приведенная выше информация задействована в таких информационных процессах, характерных для сферы ГМУ, как ведение документооборота, сбор и хранение информации, поиск и обработка информации, анализ данных, планирование и принятие управленческих решений, информирование населения [4] и др.

Вышеизложенное определяет строгие требования к обеспечению должного уровня защиты подобного типа информации. Направление защиты определяется характером информации и формой ее представления. Устанавливаются четыре класса защищенности ИС: от самого высокого (первого) к самому низкому (четвертому). Класс защиты (*К*) определяется в зависимости от уровня значимости информации (*УЗ*), обрабатываемой в ИС, и от масштаба ИС ($М_{ИС}$) [3]:

$$К = [УЗ; М_{ИС}]. \quad (1)$$

Если со временем происходит изменение масштаба ИС или в ней появляется информация с другим уровнем значимости, то требуется пересмотреть класс защищенности ИС.

Для определения масштаба ИС необходимо рассмотреть ее назначение, из каких сегментов она состоит, а также их распределенность. Масштабы ИС ГМУ РФ представлены в таблице.

Основной целью защиты информации можно считать предотвращение возможного ущерба для владельца и/или пользователя информации в результате свершения угрозы. Размер ущерба будет зависеть от формы самой угрозы и от того, какая информация подвергается угрозам. Поэтому одним из вариантов определения уровня значимости информации является оценка возможного ущерба для владельца и/или пользователя информации, возникшего в результате нарушения конфиденциальности, целостности и/или доступности информации [5]:

УЗ = [(конфиденциальность, степень ущерба)
(целостность, степень ущерба)
(доступность, степень ущерба)]. (2)

Здесь (2) оценивается вероятность свершения той или иной угрозы, а также степень возможного ущерба, которая определяется владельцем/пользователем одним из доступных методов. Можно использовать следующую градацию ущерба в зависимости от последствий в социальной, политической, международной, экономической, финансовой или иных областях деятельности организации, а также в зависимости от степени влияния реализованной угрозы на работоспособность ИС:

– высокий ущерб, если возможны существенные негативные последствия в какой-либо области деятельности, а также если ИС и/или оператор ИС (владелец информации) не могут выполнять возложенные на них функции;

– средний ущерб, если возможны умеренные негативные последствия в какой-либо области деятельности и/или ИС и/или оператор ИС (владелец информации) не могут выполнять хотя бы одну из возложенных на них функций;

– низкий ущерб, если возможны незначительные негативные последствия в какой-либо области деятельности и/или ИС и/или оператор ИС (владелец информации) могут выполнять возложенные на них функции с недостаточной эффективностью, или выполнение функций возможно только с привлечением дополнительных сил и средств [5].

Окончательно уровень значимости информации устанавливается по наивысшим значениям степени возможного ущерба,

определенным для конфиденциальности, целостности, доступности информации. Кроме того, ИС чаще всего работают с информацией разного вида, следовательно, и оценка уровня значимости выполняется отдельно для каждого вида информации.

Оценка угроз безопасности информации (*УБИ*) осуществляется по ряду факторов: оценке возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, результату анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

УБИ = [(возможности нарушителя;
уязвимости информационной системы;
способ реализации угрозы;
последствия от реализации угрозы)] [5]. (3)

Существует большое количество классификаций угроз в зависимости от используемых критериев, например:

– по аспекту информационной безопасности (основной направленности угрозы) выделяют угрозы нарушения доступности, нарушения целостности, нарушения конфиденциальности;

– по целевым объектам ИС, на которые воздействуют, различают угрозы данным, информационным процессам, программному или аппаратному обеспечению, поддерживающей инфраструктуре, носителям информации, персоналу и др.;

– по типу и характеру различают случайные/преднамеренные действия природного/техногенного характера;

– по расположению источника угроз и ее потенциалу: внешние и внутренние угрозы с низким, средним или высоким потенциалом [5].

В соответствии с моделью (2) за основу выбрана первая классификация, согласно которой выделяют: угрозы доступности, угрозы целостности и угрозы конфиденциальности.

1. Под ***доступностью*** понимают возможность за приемлемое время получить требуемую информационную услугу. В большей степени это свойство информации касается общедоступной информации, которая циркулирует в ИС ГМУ и к которой могут обращаться представители юридических лиц и физические лица [2].

К угрозам доступности можно отнести случайные ошибки операторов, штатных пользователей, системных администраторов и других лиц, обслуживающих ИС. Последствиями от реализации таких угроз могут быть внутренний отказ ИС, отказ поддерживающей инфраструктуры. Для снижения вероятности исполнения угроз доступности необходимо своевременно информировать сотрудников об изменениях в функционировании информационной системы, проводить обучение персонала, выполнять диагностику программно-технического комплекса и т.п.

2. Если рассматривать ***целостность*** как свойство информации, то это актуальность, полнота информации, отсутствие непротиворечивости, а также ее защищенность от уничтожения и несанкционированного изменения [6]. Это касается информации как общедоступной, так и с ограниченным доступом. Угрозам нарушения целостности подвержены не только данные, но и сама ИС.

Как правило, угрозы целостности связаны:

– с нарушением достоверности информации в результате нарушения правил и/или инструкций по работе с системой вследствие незнания или халатности;

– с непредумышленным или намеренным предоставлением или вводом в систему ошибочной информации.

Защита в этом случае должна быть комплексной и включать организационно-правовые и программно-аппаратные средства защиты. Например, для обеспечения достоверности и полноты информации необходимо выполнять контроль ввода новых данных, отслеживать изменения внутренней информации о ГМУ и изменений, касающихся законодательства РФ, своевременно обновляя данные. Для поддержания целостности информации и информационной системы необходимо использовать лицензионное программное обеспечение, сертифицированное аппаратное обеспечение, средства защиты от вредоносных программ, брандмауэры, средства резервного копирования, архивирования информации и т.д.

3. Для информации с ограниченным доступом важным направлением защиты является обеспечение конфиденциальности данных. ***Конфиденциальность*** – это свойство информации, характеризующее ее защиту от несанкционированного доступа. Источниками угроз конфиденциальности выступают лица, работающие в органах ГМУ или обслуживающие информационные системы ГМУ, пресса, иностранные агенты, спецслужбы, различные организации, физические лица, действующие в своих целях или целях заинтересованных лиц. Наибольшую опасность представляют собой злоумышленники, действующие внутри ГМУ и злоупотребляющие своими полномочиями [7].

Основные угрозы конфиденциальности – хищение или раскрытие информации с ограниченным доступом.

Порядок предоставления доступа к информации в ИС ГМУ определяется Правительством РФ с учетом законодательства РФ, в частности с учетом таких федеральных законов, как «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О персональных данных».

Средствами защиты информации будут:

– организационно-правовые средства, в которых определяются права, обязанности и ответственность лиц, которые могут участвовать в любых информационных процессах, характерных для деятельности органов ГМУ;

– программно-технические средства, реализующие управление доступом к конфиденциальной или закрытой информации, хранение данных в зашифрованном виде, использование электронной подписи, защиту от вредоносных программ и т.д.

Заключение

Таким образом, в статье рассмотрены информационные системы. Представленная классификация позволяет выделить крупную область ИС – государственные информационные системы. Вопросы информационной безопасности в данной области являются наиболее актуальными и требуют неотложного решения. Для государственных информационных систем определен состав с точки зрения безопасности. Представлена методика классификации информационной системы по требованиям защиты информации, что позволило выявить основные угрозы информационной безопасности и их источники. Анализ угроз позволил определить направления и способы защиты информации.

Список литературы

1. Лебедкин А.П., Капелюшный Э.Д. Применение информационных технологий в экономике и управлении // Экономика и социум. Саратов, 2017. С. 851–854.

2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 08.07.2006 (с изменениями на 14 июля 2022 года) № 149-ФЗ. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 23.08.2022).

3. Закон Российской Федерации «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 21.01.2009 (с изменениями на 30 апреля 2021 года) № 8-ФЗ. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_84602/ (дата обращения: 10.05.2021).

4. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие для вузов. М.: Горячая линия – Телеком, 2011. С. 69–71.

5. Методический документ. Меры защиты информации в государственных информационных системах [утвержден ФСТЭК России 11 февраля 2014 года]. [Электронный ресурс]. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=252834 (дата обращения: 10.05.2021).

6. Проза.ру Информационная безопасность. [Электронный ресурс]. URL: https://proza.ru/2019/08/10/1345 (дата обращения: 01.04.2021).

7. Шептура С.В. Информационная безопасность. М., 2010. [Электронный ресурс]. URL: http://www.e-biblio.ru/book/bib/01_informatika/Inform_bezopast/sg/sg.html (дата обращения: 01.04.2021).