ВОЗМОЖНЫЙ ПОДХОД К ОЦЕНКЕ УЩЕРБА ОТ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

***Нестеровский Игорь Петрович**, кандидат технических наук, г. Воронеж*
***Язов Юрий Константинович**, доктор технических наук, профессор, г. Воронеж*

Рассмотрены аспекты оценки риска в государственных информационных ресурсах (ГИС). Основное внимание уделено задачам определения вариантов оценки ущерба. Рассмотрены вопросы классификации защищенности ГИС от угроз безопасности информации. Предложена классификация видов ущерба. Детально рассмотрены особенности финансового, морального, социального и экологического ущерба для ГИС. Разработан комплекс методических правил оценки различного вида ущерба в ГИС. Показана возможность использования предложенного подхода для определения уровня значимости защищаемой информации и обоснования класса защищенности ГИС. Рассмотрены вопросы последующего обоснования требований по защите информации в ГИС.

***Ключевые слова**: угрозы безопасности информации, оценка ущерба, класс защищенности информационной системы, ГИС*

POSSIBLE APPROACH TO ASSESSMENT OF DAMAGE SUFFERED FROM A THREAT TO SECURITY OF INFORMATION BEING PROCESSED IN FEDERAL INFORMATION SYSTEMS

***Igor Nesterowskij** , Ph.D., Voronezh*
***Yuriy Yazov** , Doctor of Sciences (Tech), Professor, Voronezh*

The aspects of risk assessment in the federal information systems (FIS) are considered. The problem of determining the options to assess damage is highlighted. The questions of security classification of FIS information security threats are reviewed. The classification of types of damages is proposed. Detail the features of the financial, moral, social and environmental damage to the FIS is discussed. The set of methodological rules for evaluating various types of damage in FIS is developed. The possibility of using the proposed approach to determine the level of significance of the protected information and justification class of security FIS is shown. The questions follow substantiate claims for protection of information in the FIS are considered .

***Keywords**: information security threat, damage assessment, information system protection class, FIS*

В настоящей статье предлагается конструктивный подход к решению одной из наиболее сложных задач, которые необходимо решать при обосновании требований по защите информации в ГИС, а именно – задачи определения требуемого класса защищенности ГИС от угроз безопасности информации. Необходимость классификации ГИС определена нормативным правовым актом ФСТЭК России[1] (далее по тексту – Требования о защите информации).

Предлагаемый подход ориентирован на ГИС, в которых отрабатывается информация ограничен-

1 НПА «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденный приказом ФСТЭК России от 11 февраля 2013 г. № 17.

ного доступа, не содержащая сведений, составляющих государственную тайну, а также на ГИС, в которых защищается информация, не относящаяся к информации ограниченного доступа, но нарушение безопасности которой может негативно повлиять на деятельность органа власти или государственной организации (предприятия), либо иная информация, не относящаяся к информации ограниченного доступа, нарушение целостности или доступности которой может нанести ущерб ее обладателю.

Класс защищенности – это категория классификации, устанавливаемая для информационной системы в интересах сопоставления требуемого уровня защищенности обрабатываемой в ней информации с определенной совокупностью требований по защите информации. Класс защищенности ГИС, в соответствии с Требованиями о защите информации, определяется масштабом ГИС (федеральная, региональная или объектовая) и значимостью обрабатываемой в ней информации, которая, в свою очередь, определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации. Задача оценки ущерба усложняется тем, что нарушения безопасности информации, обрабатываемой в ГИС, могут приводить к ущербу в социальной, политической, международной, экономической, финансовой или иных областях деятельности, причем в каждой из этих областей деятельности возможно причинение одного из следующих видов ущерба: финансового, экономического, материального, экологического, социального, морального и их сочетаний. Как правило, экономический и материальный ущербы могут быть пересчитаны в финансовый и поэтому далее как самостоятельные виды ущерба не рассматриваются. Остальные виды ущерба могут быть охарактеризованы следующим образом.

Финансовый ущерб, в основном, обусловлен:

- возможностью потерь финансовых средств, в том числе неполучением ожидаемой прибыли;

- необходимостью дополнительных затрат на выплату штрафов (неустоек) и компенсаций гражданам (клиентам, сотрудникам);

- необходимостью дополнительного финансирования запланированных работ и работ, связанных с ликвидацией последствий нарушений безопасности информации в ГИС (в том числе закупка и/или разработка программного и/или аппаратного обеспечения, модернизация системы защиты информации).

Экологический ущерб обусловлен возможностью возникновения ситуаций, при которых создается опасность жизни и здоровью граждан вследствие загрязнения окружающей среды радиоактивными, токсическими или болезнетворными биологическими материалами.

Социальный ущерб может быть обусловлен возможностью возникновения (нарастания) социальной напряженности в обществе, которая проявляется в возрастании количества жалоб в органы власти и местного самоуправления, в появлении публикаций с критикой организаций и органов власти, в активизации выступлений общественных организаций и политических партий, в проведении демонстраций, организации и осуществлении акций гражданского неповиновения.

Моральный ущерб, в основном, обусловлен возможностью:

- снижения государственного престижа на международном уровне;

- снижения престижа федеральных органов власти, органов власти субъектов Российской Федерации и органов местного самоуправления;

- дискредитации руководителей государственных структур;

- нарушения деловой репутации государственных организаций;

- нанесения морального вреда (оскорбление, публикация ложных сведений об организации, органе власти, сведений личного характера, персональных данных) гражданам, сотрудникам государственных организаций и органов власти.

Величину (степень) ущерба, в соответствии с Требованиями о защите информации, следует оценивать качественно по вербальной шкале. При этом предлагается к трем определенным Требованиями о защите информации градациям (высокая, средняя и низкая степень ущерба) ввести еще одну – минимальная степень. Степень ущерба признается минимальной, если обладателем информации (заказчиком) и (или) оператором ущерб от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) не может быть определен, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

Рассмотрим возможные варианты определения степени ущерба для введенных в рассмотрение видов ущерба.

Оценка финансового ущерба производится с учетом характера информации ограниченного доступа, содержания несанкционированных действий с защищаемой информацией и уровня последствий от нарушения защищаемой информации в ГИС (федерального, регионального, объектового). При этом информация ограниченного доступа подразделяется на финансово-экономическую, административно-управленческую и технологическую. Для каждой такой информации выявляются возможные несанкционированные действия и далее для каждого действия оценивается возможный ущерб. Предлагаемые правила такой оценки приведены в таблице 1.

Экологический ущерб оценивается в том случае, когда вследствие нарушений доступности или целостности системного, прикладного программного обеспечения или используемых данных может произойти нарушение функционирования ГИС и с развитием чрезвычайной ситуации, связанной с гибелью людей или нарушением условий их жизнедеятельности; если же экологический ущерб приводит лишь к финансовым потерям, то он должен учитываться при определении финансового ущерба (необходимость дополнительного финансирования работ, связанных с ликвидацией последствий нарушений безопасности информации в ГИС) и отдельно не рассматривается.

Определение величины (степени) экологического ущерба производится на основе данных о масштабе прогнозируемой чрезвычайной ситуации. Предлагаемые правила оценки возможного экологического ущерба приведены в таблице 2.

Оценка величины (степени) социального ущерба основывается на определении возможного уровня социальной напряженности, вызванной сбоями или недостатками в работе органа власти или организации (предприятия), влияющими на жизнь людей, обеспечение их прав и свобод, или связанной с незаконным распространением персональных данных людей и иной подлежащей защите информации без согласия физических и юридических лиц.

Непосредственными причинами сбоев и недостатков являются:

- нарушение функционирования ГИС или уничтожение информации и связанное с этим существенное замедление работы органа власти, организации (предприятия);

- несанкционированное изменение данных, хранящихся в ГИС, и выдача гражданам или организациям неверных данных;

- кража и несанкционированное распространение информации, обладателями которой являются физические или юридические лица.

Величина (степень) социального ущерба определяется в зависимости от последствий, к которым может привести реализация угроз безопасности информации и от уровня (предприятие, муниципальные органы, органы власти субъектов Российской Федерации, федеральные органы власти), на котором могут проявиться эти последствия в результате реализации угроз безопасности информации в ГИС.

Предлагаемые правила оценки степени социального ущерба приведены в таблице 3.

Оценка величины (степени) морального ущерба основывается на определении того, чьи интересы могут быть затронуты в результате утечки информации (в том числе персональных данных), нарушения ее целостности и доступности или нарушения функционирования ГИС в целом с существенным затруднением выполнения органом власти или организации своих функций.

Величина (степень) морального ущерба зависит от вида и масштаба последствий реализации угроз безопасности информации. Предлагаемые правила ее оценки приведены в таблице 4.

В заключение необходимо отметить, что при оценке величины (степени) возможного ущерба следует полагать, что несанкционированные действия осуществляются относительно всей защищаемой информации ГИС, то есть получаемая оценка ущерба должна являться оценкой сверху (полагается, что наносится максимально возможный ущерб).

Если реализация угроз безопасности информации может привести к одновременному осуществлению двух и более несанкционированных действий (например, хищение информации ограниченного доступа и модификация иной информации, нарушение безопасности которой может нанести ущерб ее обладателю или негативно повлиять на его деятельность), то необходимо применять следующее правило: результирующий суммарный ущерб соответствует ущербу на одну категорию выше, чем максимальный из всех парциальных ущербов.

Предложенный в настоящей статье подход может быть использован при проведении работ по защите информации в ГИС для решения задачи определения уровня значимости защищаемой информации, обоснования класса защищенности ГИС в интересах последующего обоснования требований по защите обрабатываемой в них информации.

Таблица 1.

Предлагаемые правила оценки возможного финансового ущерба от реализации угроз безопасности информации

Содержание несанкционированных действий с защищаемой информацией	Вид защищаемой информации											
	Информация ограниченного доступа									Иная защищаемая информация		
	Финансово-экономического характера			Административно-управленческого характера			Технологического характера			Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне
	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне			
Нарушение конфиденциальности информации	Низкий	Средний	Высокий	Минимальный	Низкий	Средний	Минимальный	Низкий	Низкий	Минимальный	Низкий	Низкий
Нарушение целостности информации	Низкий	Средний	Высокий	Минимальный	Низкий	Средний	Минимальный	Низкий	Низкий	Минимальный	Минимальный	Низкий
Нарушение доступности информации	Минимальный	Низкий	Средний	Минимальный	Минимальный	Низкий	Минимальный	Низкий	Низкий	Минимальный	Минимальный	Низкий

Таблица 2.

Предлагаемые правила оценки возможного экологического ущерба от реализации угроз безопасности информации

Последствия от реализации угроз безопасности информации	Масштаб чрезвычайной ситуации	Возможный экологический ущерб
Территория, на которой может сложиться чрезвычайная ситуация и будут нарушены условия жизнедеятельности людей, не выходит за пределы территории объекта и количество людей, которые могут погибнуть или получить ущерб здоровью (далее - количество пострадавших), не может превысить 10 человек	Чрезвычайная ситуация локального характера	Минимальный
Территория, на которой может сложиться чрезвычайная ситуация и будут нарушены условия жизнедеятельности людей, не выходит за пределы территории одного поселения или внутригородской территории города федерального значения и количество людей, которые могут погибнуть или получить ущерб здоровью (далее - количество пострадавших), не может превысить 50 человек	Чрезвычайная ситуация муниципального характера	Низкий
Территория, на которой может сложиться чрезвычайная ситуация и будут нарушены условия жизнедеятельности людей, не выходит за пределы территории одного субъекта Российской Федерации, при этом количество пострадавших может составить свыше 50 человек, но не более 500 человек	Чрезвычайная ситуация регионального характера	Средний
Территория, на которой может сложиться чрезвычайная ситуация выходит за пределы одного субъекта Российской Федерации и будут нарушены условия жизнедеятельности более чем 500 человек	Чрезвычайная ситуация федерального характера	Высокий

Таблица 3.

Правила оценки возможного социального ущерба от реализации угроз безопасности информации

Содержание несанкционированных действий с защищаемой информацией	Возможное недовольство населения, выражаемое в жалобах в органы власти и публикациях в прессе			Возможное подключение к разрешению ситуации выборных органов власти			Возможные выступления населения в виде пикетов и демонстраций, проведение акций гражданского неповиновения		
	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне
Неправомерные доступ, копирование, предоставление или распространение информации (нарушение конфиденциальности информации)	Низкий	Средний	Средний	Низкий	Средний	Высокий	Низкий	Средний	Высокий
Неправомерные уничтожение или модифицирование информации (нарушение целостности информации)	Минимальный	Низкий	Средний	Низкий	Средний	Средний	Мини-мальный	Средний	Высокий
Неправомерное блокирование информации (нарушение доступности информации)	Минимальный	Низкий	Низкий	Мини-мальный	Низкий	Низкий	Мини-мальный	Низкий	Средний

Таблица 4

Правила оценки возможного морального ущерба от реализации угроз безопасности информации

Содержание несанкционированных действий с защищаемой информацией	Снижение престижа организации, органа власти или государства в целом			Дискредитация или нарушение деловой репутации должностных лиц. Причинение морального вреда гражданам, сотрудникам государственных организаций и органов власти (оскорбление, публикация ложных сведений, сведений личного характера)		
	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне	Последствия проявляются на объектовом уровне	Последствия проявляются на региональном уровне	Последствия проявляются на федеральном уровне
Неправомерные доступ, копирование, предоставление или распространение информации (нарушение конфиденциальности информации)	Низкий	Средний	Высокий	Минимальный	Средний	Высокий
Неправомерные уничтожение или модифицирование информации (нарушение целостности информации)	Минимальный	Средний	Высокий	Минимальный	Средний	Средний
Неправомерное блокирование информации (нарушение доступности информации)	Минимальный	Низкий	Средний	Минимальный	Низкий	Средний

Литература:

1. Язов Ю.К., Сердечный А.Л., Шаров И.А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60
2. Шварцкопф Е.А., Ноздрачева Л.С., Нестеровский И.П. Регулирование полосы неравномерности общего риска при синтезе распределенных компьютерных систем // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем. 2014. Т. 6. № 4. С. 39-49.

References:

1. Iazov Iu.K., Serdechny`i` A.L., Sharov I.A. Metodicheskii` podhod k ocenivaniiu e`ffektivnosti lozhny`kh informatcionny`kh sistem // Voprosy` kiberbezopasnosti. 2014. № 1 (2). S. 55-60
2. Shvartckopf E.A., Nozdracheva L.S., Nesterovskii` I.P. Regulirovanie polosy` neravnomernosti obshchego riska pri sinteze raspredelenny`kh komp`iuterny`kh sistem // Upravlenie informatcionny`mi riskami i obespechenie bezopasnosti infokommunikatcionny`kh sistem. 2014. T. 6. № 4. S. 39-49.