doi:10.18720/SPBPU/2/id25-351

Голованов Владимир Борисович, заместитель начальника аналитического отдела АО «Информационные технологии и коммуникационные системы», Москва, Россия, Vladimir.Golovanov@infotecs.ru

РИСКИ КИБЕРБЕЗОПАСНОСТИ И ИХ УЧЕТ В ПРОЦЕССАХ ПРОЕКТИРОВАНИЯ ЗДАНИЙ

Аннотация. В статье обсуждаются вопросы, связанные с учетом факторов рисков информационной безопасности, включая киберриски, при проектировании зданий и сооружений. Информатика в современных условиях пронизывает все производственные и управленческие процессы. Объемы создаваемой и обрабатываемой информации ежегодно растут. При этом информация как объект защиты требует дифференцированного подхода при применении защитных мер. Игнорирование установленных норм сопряжено как с ростом проектных рисков, так и с ростом рисков надлежащей эксплуатации зданий и сооружений, а также внеплановой их реконструкции и сопутствующих непредусмотренных издержек (временных, финансовых и других), а также репутационных потерь. Показаны пути практического решения рассматриваемой задачи, включая последовательность действий при проектировании зданий и сооружений, и место «классическому» менеджменту рисков информационной безопасности в этом процессе.

Ключевые слова: виды информации, проектирование зданий, информационная безопасность, контролируемая зона.

Golovanov Vladimir Borisovich, Deputy Head of Analytical Unit, Joint Stock Company «Information Technologies and Communication Systems», Moscow, Russia, Vladimir.Golovanov@infotecs.ru

CYBERSECURITY RISKS AND THEIR CONSIDERATION IN BUILDING DESIGN PROCESSES

Abstract. The article discusses the issues related to the consideration of information security risk factors, including cyber risks, in the design of buildings and structures. Informatics in modern conditions permeates all production and management processes. The volumes of created and processed information are growing annually. At the same time, information, as an object of protection, requires a differentiated approach in the application of protective measures. Ignoring the established norms is associated with both the growth of design risks and the growth of risks of proper operation of buildings and structures, as well as their unscheduled reconstruction and associated unintended costs (time, financial and other), as well as reputational losses. The ways of practical solution of the problem under consideration are shown, including the sequence of actions in the design of buildings and structures, and the place of “classical” information security risk management in this process.

Keywords: types of information, building design, information security, controlled area.

Уже более 10 лет термин кибербезопасность насаждается из-за рубежа в российскую практику и на настоящее время проник во все сферы производственной и повседневной деятельности, включая деятельность по нормативному регулированию.

При этом сам термин «кибербезопасность» определяет часть сущности понятия «безопасность информации», что закреплено в международных и российских национальных стандартах.

Например, в международном стандарте ISO/IEC 27032 «Руководство по кибербезопасности» [1] понятие «*кибербезопасность*» определено как «*сохранение конфиденциальности, целостности и доступности информации в киберпространстве*», включая примечание к нему, в котором отмечается, что «*кроме того, могут быть востребованы и другие свойства безопасности, такие как аутентичность, подотчетность, неотказуемость и надежность.*». А в российском национальном стандарте ГОСТ Р 50922 [2] понятие «безопасность информации» определяется следующим образом: «*Состояние защи-*

щенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность».

То есть, два, казалось бы, совершенно различных термина имею практически идентичное определение, что очень важно с практической точки зрения, а именно: все требования в РФ, введенные и обязательные для задач обеспечения «*безопасности информации*» или еще именуемые «*защитой информации*», являются актуальными и в тех случаях, когда речь идет о «*кибербезопасности*» и производных от нее задач (киберриски, кибер-угрозы и т.п.).

Другим важным выводом из отмеченного является то, что объектом защиты в каждом случае выступает такая сущность, как «*информация*» в различных формах и видах её представления.

А какие виды информации выделяются с точки зрения норм права [3] и практики? Это следующие две категории: «*информация ограниченного доступа*», подлежащая защите в соответствии с требованиями законодательства, доступ к которой ограничен в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, и «*общедоступная информация*», доступ к которой не может быть ограничен опять же в соответствии с требованиями законодательства . Рисунок 3.1 иллюстрирует данный факт.

Рисунок 3.1 – Виды информации

Дополнительно следует отметить, что между информацией ограниченного доступа и открытой информацией есть еще одна категория, так называемая чувствительная информация или служебная тайна. Это та информация, которая не подпадает под нормативные ограничения, но и не может быть открытой в силу ряда служебных, деловых или иных подобных причин. Самый простой пример: электронные письмо или письмо на бумажном носителе о намерении выйти из проекта или о желании заключения новой сделки. Пока еще нет ни коммерческих параметров и как таковой «*коммерческой тайны*», но несанкционированное раскрытие третьим лицам подобной информации может иметь огромные последствия. При этом на фоне внутрироссийских и международных событий 2022 года и последующих годов обострилась проблема сохранности любой непубличной информации. Это побудило многие российские ведомства издать приказы об обеспечении защиты служебной информации (информации «для служебного пользования», ДСП), не подпадающей под ограничения действующего законодательства, для надлежащей ее защиты от несанкционированного разглашения.

Таким образом, следует учитывать требования по защите для всех категорий непубличной информации, как для государственной тайны, так и при обработке информации ограниченного доступа (*ИОД*), а также сведений *ДСП* и им подобных.

В целом защита информации включает следующе две крупные группы требований:

1) требования к мерам, связанным с применением программных и программно-аппаратных средств защиты, иначе - средств безопасности информационных технологий (ИТ-средства, средства кибербезопасности);

2) требования к мерам, не связанным с ИТ-средствами безопасности, включая меры противодействия утечкам информации по техническим каналам и силовым деструктивным воздействиям на средства вычислительной техники, каналы связи и каналообразующее оборудование и т.п.

Вторая группа требований включает и требования к помещениям и их расположению, применению специальных материалов при строи-

тельстве и отделке помещений, возведению дополнительных конструкций и т.п.

Что же касается риск-менеджмента, то в случае наличия потребности в обработке на объектах организации сведений, составляющих «*государственную тайну*», следует неукоснительно исполнять требования Государства, сформулированные в ряде специальных нормативных документов, с привлечением компетентных подрядчиков, а вопросы риск-менеджмента в этом случае не уместны. Данные требования включают ряд положений, имеющих отношение к физической защищённости зданий и сооружений, защищенности и расположению помещений, где обрабатывается защищаемая информация, соблюдению размеров так называемых «контролируемых зон», типу и порядку размещения каналов связи, системам электропитания, вентиляции и другим инженерным коммуникациям и т.п.

Если осуществляется обработка *ИОД*, подлежащая защите в соответствии с требованиями законодательства РФ, или *ДСП* и аналогичные сведения, то должны исполняться соответствующие требования Регуляторов (ФСБ России, ФСТЭК России, Роскомнадзора и др.), ведомственные приказы по защите конфиденциальной информации и служебных сведений, а в дополнение к их исполнению и с учетом специфики деятельности организации возможна дополнительная оценка в рамках «классического» риск-менеджмента ИБ, например, в соответствии с ISO/IEC 27005 [4] или по методическим рекомендациям органов регулирования [5].

При оценке в рамках «классического» риск-менеджмента ИБ может быть использована схема оценки по ISO/IEC 27005 [4], показанная на рисунке 3.2, которая предусматривает последовательную итерационную деятельность на соответствующих этапах работ и использование необходимых для их выполнения данных и экспертных оценок, а также шкал и метрик пороговых значения принятия/непринятия рисков безопасности. В случае, если риски оценены как неприемлемые, должны выбираться меры защиты информации, организационные или технические, а в определенных случаях и касающиеся требований к физической среде обработки информации. В приложении к стандарту приведены примеры различных сценариев оценки рисков, включая:

«Событийный подход», «График зависимости активов», «Модели SFDT» и т.п.

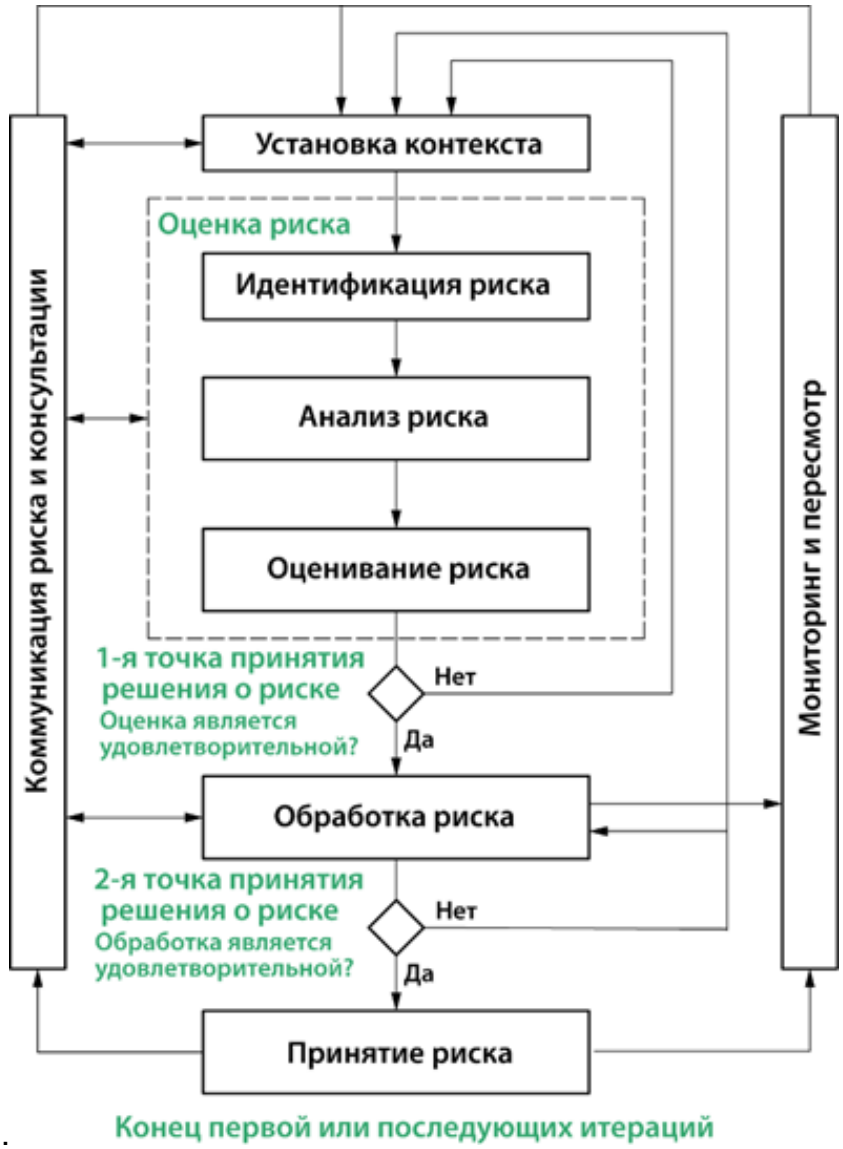

Рисунок 3.2 – Процесс управления рисками информационной безопасности по ИСО/МЭК 27005

Методические рекомендации российского регулятора [5], преследуя те же результаты, изначально опираются на физическое размещение и расположение средств обработки информации. Рисунок 3.3, заимствованный из первоисточника, иллюстрирует рекомендуемый первый шаг при оценке угроз безопасности, а именно – описание расположения и границ обработки защищаемой информации и, следовательно, и границ оценки угроз и рисков. В данном случае граница мо-

делирования угроз безопасности информации – это совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации в соответствии с едины-ми правилами и процедурами, а также контроль за реализованными мерами защиты информации.

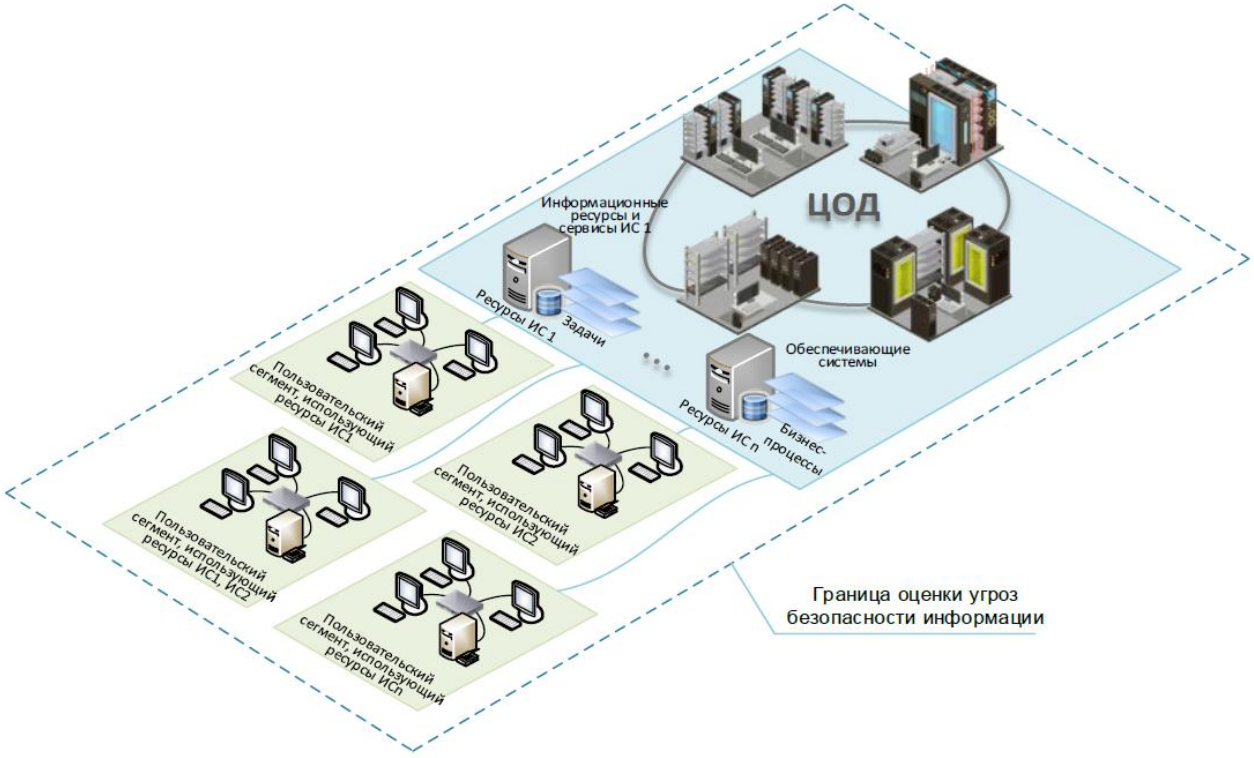

Рисунок 3.3 – Оценка угроз безопасности информации в информационной инфраструктуре на базе центра обработки данных

В конечном итоге работы по анализу применимых требований по защите информации должны завершится перечнем рекомендаций проектировщикам, а также самой организации, которая в будущем будет эксплуатировать объект. На некоторые помещения могут быть затребованы технические паспорта безопасности, разрабатываемые в соответствии с требованиями [6].

Таким образом, подводя итоги рассмотрения вопроса учета рисков кибербезопасности в процессах проектирования зданий, следует отметить , что:

1) виды обрабатываемой информации или категория защищаемой информации – главный критерий применимости и, при возможности, критерий предпочтительного подхода к оценке рисков;

2) при обработке на объекте сведений, составляющих государственную тайну, при проектировании и в процессе строительства зданий и сооружений следует привлекать экспертную организацию;

3) при обработке на объекте сведений конфиденциального характера необходимо запросить у Заказчика строительства сведения по планам размещения и необходимости учета помещений в соответствии с установленными требованиями по защите информации ограниченного доступа, обработать эти сведения в соответствии с действующим законодательством, после чего дополнительно могут быть задействованы различные подходы по управлению киберрисками или рисками информационной безопасности.

Библиографический список

1. ISO/IEC 27032–2012 Information technology — Security techniques — Guidelines for cybersecurity.

2. ГОСТ Р 50922–2006 Защита информации. Основные термины и определения.

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Ст. 5 «Информация как объект правовых отношений».

4. ISO/IEC 27005–2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

5. Методический документ. «Методика оценки угроз безопасности информации», утв. ФСТЭК России 5 февраля 2021 г.

6. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утв. приказом ФСТЭК России от 29 апреля 2021 г. N 77.