ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59516— 2021

Информационные технологии

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Правила страхования рисков информационной безопасности

(ISO/IEC 27102:2019, NEQ)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский университет «Московский институт электронной техники» и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 420-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 27102:2019 «Менеджмент информационной безопасности. Рекомендации по страхованию кибер-рисков» (ISO/IEC 27102:2019 «Information security management — Guidelines for cyber-insurance», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Инциденты информационной безопасности (ИБ) могут случиться в любой момент времени и иметь различные последствия для организации или физического лица. Например, активы организации, в том числе информационные, могут подвергаться атакам, которые становятся все более объемлющими, целенаправленными и сложными.

В целях ослабления последствий, возникающих в результате инцидентов ИБ, в дополнение к принятым в соответствии с ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 27002 организационным и техническим мерам обеспечения ИБ, следует внедрять страхование рисков ИБ.

Страхование рисков ИБ не рассматривается как альтернатива эффективной системе менеджмента информационной безопасности информации (СМИБ) и не может исключить необходимость разработки планов реагирования на инциденты ИБ, создания системы обучения персонала и принятия других организационных и технических мер по защите информационных активов.

Страхование рисков ИБ следует рассматривать как важный компонент СМИБ по противодействию угрозам ИБ и повышению устойчивости бизнеса.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Правила страхования рисков информационной безопасности

Information technology. Information security management. Guidelines for cyber-insurance

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит правила, применяемые при принятии решения о приобретении услуг страхования рисков информационной безопасности (ИБ)[1)].

Настоящий документ содержит рекомендации по:

- совершению покупки услуг страхования рисков ИБ как способа распределения риска ИБ со страховщиком;
- управлению последствиями инцидентов ИБ с помощью средств страхового покрытия;
- организации коммуникации между страхователем и страховщиком с целью поддержки андеррайтинга, мониторинга и претензионной работы, связанной с поддержкой договорных отношений между сторонами страхования рисков ИБ;
- применению СМИБ при взаимодействии со страховщиком.

Настоящий стандарт применим при планировании покупки услуг страхования рисков ИБ организациями всех типов, размеров и характера деятельности, а также физическими лицами.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27003 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27004 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный

[1)] Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.

Издание официальное

стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р ИСО/МЭК 27000, а также следующие термины с соответствующими определениями:

3.1 **договор страхования:** Соглашение между страхователем и страховщиком, в соответствии с условиями которого одна сторона (страховщик) обязуется за обусловленную договором плату (страховую премию) при наступлении предусмотренного в договоре события (страхового случая) возместить другой стороне (страхователю) или иному лицу, в пользу которого заключен договор (выгодоприобретателю), причиненные вследствие этого события убытки в застрахованном имуществе либо убытки в связи с иными имущественными интересами страхователя (выплатить страховое возмещение) в пределах определенной договором суммы (страховой суммы).

3.2 **страховой полис:** Документ, подтверждающий заключение договора страхования, выдаваемый страховой компанией страхователю, содержащий указание на субъекты страховых отношений и существенные условия договора страхования, например, вид, объект, начало и конец действия страхования, размер страховой суммы, сведения о страхователе, страховщике и другие условия.

3.3

страхователи: Юридические лица и дееспособные физические лица, заключившие со страховщиками договоры страхования либо являющиеся страхователями в силу закона.

[[1], статья 5]

3.4

страховщики: Страховые организации и общества взаимного страхования, созданные в соответствии с законодательством Российской Федерации для осуществления деятельности по страхованию, перестрахованию, взаимному страхованию и получившие лицензии на осуществление соответствующего вида страховой деятельности в установленном порядке.

[[1], статья 6]

3.5

страхование: Отношения по защите интересов физических и юридических лиц, Российской Федерации, субъектов Российской Федерации и муниципальных образований при наступлении определенных страховых случаев за счет денежных фондов, формируемых страховщиками из уплаченных страховых премий (страховых взносов), а также за счет иных средств страховщиков.

[[1], статья 2]

4 Структура настоящего стандарта

Обзор и рекомендации по страхованию рисков ИБ приведены в разделах 5—8.

В разделе 5 содержится общая информация и описание отрасли страхования рисков ИБ. В разделе 6 приведено описание рисков ИБ, которые могут быть покрыты страхованием. Положения разделов 5 и 6 касаются как страхователей, так и страховщиков. В разделе 7 приведено описание типовой деятельности по оценке рисков ИБ, которую страховщик обычно проводит в рамках андеррайтинга, в разделе 8 описывается порядок использования СМИБ страхователя для подготовки исходных данных, информации и документов, передаваемых страховщику.

В приложении А представлен перечень документов, создаваемых в рамках СМИБ, которые может запросить страховщик при заключении договора, так и при исполнении договорных отношений.

5 Обзор услуг страхования рисков информационной безопасности и договор страхования

5.1 Страхование рисков информационной безопасности

Страхование рисков ИБ является одним из способов управления ИБ, который может компенсировать застрахованному лицу финансовые потери, связанные с инцидентами ИБ.

Услуга страхования рисков ИБ предоставляется страховщиком, который страхует риски ИБ, и принимает на себя часть ответственности страхователя, тем самым гарантируя выплату в случае возникновения убытков или ущерба.

Страхование рисков ИБ призвано компенсировать потери, вызванные широким спектром инцидентов ИБ, связанных с утечкой информации, остановкой бизнес-процессов и деградацией сетевой инфраструктуры.

Внедрение страхования рисков ИБ позволит обеспечить страхователю:

- минимизацию последствий инцидента информационной безопасности;
- финансирование возмещения крупного ущерба;
- содействие восстановлению штатной деятельности;
- повышение устойчивости бизнес процессов страхователя к инцидентам информационной безопасности.

Страхователь обязан продемонстрировать страховщику соответствие СМИБ покрываемому риску ИБ, установленному договором страхования.

5.2 Договор страхования рисков информационной безопасности

Договорные условия страхования рисков ИБ приведены в полисе страхования рисков ИБ. Полис страхования рисков ИБ может быть, как самостоятельным полисом, так и включаться в качестве специальных индоссаментов в составе полисов общей ответственности, имущественного или иного страхования.

Страховое покрытие полиса страхования рисков ИБ охватывает широкий спектр угроз ИБ, способных нанести вред страхователю. Нанесение вреда возможно в результате потери конфиденциальности, целостности или доступности информации, или потери работоспособности информационных систем к обеспечению потребностей бизнеса независимо от точной причины инцидента ИБ и от того, был ли он случайным или преднамеренным. Покрытие полиса страхования рисков ИБ зависит от конкретного продукта страхования, не стандартизировано и варьируется в зависимости:

- от потребности страхователя;
- ограничений, установленных в нормативных правовых актах;
- общепринятых рыночных практик;
- бизнес-решений страховщика.

Полисы страхования рисков ИБ покрывают расходы, связанные с инцидентами ИБ, и могут обеспечивать доступ к услугам, которые поддерживают деятельность страхователя после инцидента ИБ. К таким услугам относятся: оценка ущерба, понесенного в результате инцидента ИБ; разработка планов реагирования на инциденты ИБ и восстановления работоспособности информационных систем; правовая экспертиза; судебная экспертиза; помощь при установлении связей с общественностью; помощь по уведомлению клиентов; а также помощь по восстановлению бизнес-процессов после инцидента ИБ.

Полис страхования рисков ИБ предполагает возможность частичного или полного покрытия внутренних и внешних затрат, связанных с реагированием на инцидент ИБ, которое варьируется в зависимости от конкретного.

6 Риски информационной безопасности и страховое покрытие

6.1 Процесс управления рисками и страхование рисков информационной безопасности

Заключение договора страхования рисков ИБ часто позволяет страхователю уменьшить вред от инцидентов ИБ путем его разделения со страховщиком.

Организация должна быть защищена от инцидентов ИБ путем использования процессов предотвращения, идентификации, обработки и реакции на инциденты ИБ.

Процесс управления рисками ИБ должен включать корректное отображение их в поле терминов, используемых в бизнесе для того, чтобы выделить и оценить последствия от инцидентов ИБ. Подобное отображение позволит сделать более достоверные выводы для управления рисками ИБ различными способами:

- уклонение;
- устранение угрозы;
- изменение вероятности наступления последствий риска;
- удержание рисков;
- передача рисков третьим лицам, например, страховщику.

Управленческие решения, связанные с обработкой рисков ИБ, должны учитывать использование услуг страхования для их минимизации. Одним из результатов процесса менеджмента ИБ является информация о возможных рисках ИБ, а также возможных последствиях. Данный процесс реализуется целью обеспечения соответствия стратегии по обработке рисков ИБ, а также критериев их оценки условиям договора о страховании рисков ИБ.

6.2 Инциденты информационной безопасности

6.2.1 Общие положения

Инцидент ИБ происходит там, где риск ИБ становится реальностью и приводит к существенному вреду в результате потери конфиденциальности, целостности, доступности информационных активов.

Источником инцидента ИБ являются угрозы ИБ, которые используют уязвимости СМИБ и информационных систем. СМИБ и информационные системы подвержены атакам типа «отказ в обслуживании», вторжение в сеть организации, распространение вредоносных программ, ненадлежащее использование информации или информационных систем и вымогательство.

Кроме того, существуют и другие источники угроз ИБ, такие как ошибки, упущения и неисправности информационных систем и сетей. Организация должна выявлять соответствующие угрозы ИБ в свете своего делового и технологического контекста.

Инцидент ИБ может быть вызван непреднамеренной ошибкой персонала или системным сбоем и может повлиять на непрерывность деловой деятельности страхователя и, как следствие, потребовать ремонта или замены неисправных узлов.

6.2.2 Инциденты информационной безопасности

Инциденты ИБ, связанные с внутренними или внешними источниками угроз ИБ, относятся к одной или одновременно нескольким из следующих категорий:

- отказ информационной системы: информационная система или сеть страхователя функционирует некорректно и/или наносит вред системе третьего лица или информационной системе поставщика, что отрицательно влияет на непрерывность бизнес-процессов самой организации, на производительность труда;
- нарушение конфиденциальности информации: информация, хранящаяся в информационной системе страхователя (управляемой самой организацией или третьей стороной), была украдена или раскрыта;
- нарушение целостности или доступности информации: информация, находящаяся в информационной системе страхователя (управляемой самой организацией или третьей стороной) была повреждена или удалена;
- прочая вредоносная деятельность: неправомерное использование информационной системы страхователя с целью нанесения вреда (кибер-буллинг, осуществляемый при помощи социальных платформ или фишинг) или незаконное получение прибыли (кибер-мошенничество);
- человеческий фактор: ситуация, в которой человек совершил непреднамеренное воздействие на элементы информационных активов, сеть или информацию.

Основные причины инцидентов могут быть отнесены к трем категориям: ошибкам людей, отказам систем или процессов.

Каждый класс перечисленных инцидентов может быть покрыт страхованием рисков ИБ.

6.3 Влияние инцидентов информационной безопасности на бизнес и страховые убытки

6.3.1 Обзор

В результате инцидента ИБ может нанесен, в том числе значительный, вред организации. Этот вред может включать потерю или компрометацию персональных данных, потерю доходов, нарушению

цепочек поставок и/или прерыванию деловой деятельности. В результате инцидента ИБ и после него организация может столкнуться со значительными расходами на восстановление деятельности, проведение расследований и урегулирование штрафных санкций и ведение судебных дел.

Некоторые последствия инцидентов ИБ могут быть оценены количественно, например, сокращение или приостановление продаж, упущенная выгода, стоимость антикризисного управления, судебно-медицинские расследования, судебные иски и компенсация, уведомления деловых партнеров и клиентов, нормативные расследования, штрафы, оплата услуг адвокатов, консультантов и специалистов по связям с общественностью, стоимость корректирующих мер.

Некоторые виды вреда сложно подсчитать количественно, к примеру, вред репутации организации, влияние потери управления, моральный вред сотрудникам и прочему персоналу, вред, вызванный утечкой коммерческой тайны и прочие нарушения прав интеллектуальной собственности.

Инцидент ИБ, затрагивающий организацию, также может произойти у поставщика или другой третьей стороны, оказывающей обеспечивающие услуги.

6.3.2 Типы страхового покрытия

Страхование рисков ИБ может покрывать основные виды вреда, включая:

а) ответственность страхователя (6.3.3);

б) затраты по реагированию на инцидент (6.3.4);

в) затраты по предотвращению вымогательства (6.3.5);

г) затраты, вызванные прерыванием деловой деятельности (6.3.6);

д) штрафы и пени, вызванные нарушением предписаний нормативных правовых актов (6.3.7);

е) штрафы и пени, вызванные нарушением договоров (6.3.8);

ж) затраты на восстановление информационных систем (6.3.9).

Примечания

1 Перечисление д) применимо не во всех случаях.

2 Список типов страхового покрытия может быть дополнен дополнительными пунктами ввиду постоянного развития отрасли страхования рисков ИБ.

Страхователь должен выбирать те типы покрытия, которые наиболее полным образом покрывают перечень идентифицированных рисков ИБ.

6.3.3 Ответственность страхователя

Инцидент может привести к наступлению ответственности страхователя по возмещению убытков третьим сторонам.

Такая ответственность может включать:

- вред, причиненный страхователю или другим организациям;
- нарушение защиты персональных данных клиента или поставщика.

6.3.4 Затраты по реагированию на инциденты

6.3.4.1 Обзор

В результате инцидента ИБ могут возникнуть различные расходы на реагирование. Страхование рисков ИБ обычно обеспечивает покрытие некоторых, но не обязательно всех расходов. В 6.3.4.2—6.4.8 представлены типовые примеры таких расходов.

Примечание — Некоторые страховые компании могут не включать определенные типы покрытия в перечень своих услуг, ввиду установившихся бизнес-практик данной отрасли.

6.3.4.2 Утрата, кража или повреждение данных

Инцидент ИБ может привести к утечке информации. Коммерческая или и иная информации страхователя может обесцениваться. Типичный пример утечки информации, приводящей к значительному вреду для страхователя — получение конкурентами несанкционированного доступа к коммерческой тайне или информации об изобретении до публичного раскрытия в качестве патента. Утечка персональных данных может приводить к штрафам и другим расходам, связанным с урегулированием конфликта с физическими лицами.

Инцидент ИБ может привести к нарушению целостности или доступности информации, работоспособности информационных систем, а также причинить вред другим активам страхователя. Понесенный вред может отрицательно сказаться на эффективности деловой деятельности страхователя, включая внутренние операции, предоставление услуг, производственные и эксплуатационные процессы.

В результате инцидента ИБ информация страхователя может быть повреждена или похищена. Это может повлечь за собой затраты на замену или восстановление поврежденной информации путем ее восстановления, обновления, воссоздания или замены до приемлемого состояния.

Похищенная информация имеет ценность для страхователя, и эта ценность должна рассматриваться как размер вреда, полученного организацией в случае, если такая информация не может быть восстановлена. Страхователь может также понести расходы при попытке восстановить похищенную информацию. Помимо прочего, несанкционированное копирование конфиденциальной информации также может снизить ее ценность.

Особым случаем является утрата или кража интеллектуальной собственности, например, коммерческой тайны изобретения до раскрытия в качестве патента и защищенного авторским правом. Утраченная интеллектуальная собственность имеет текущую и будущую стоимость для страхователя, и эта стоимость должна рассматриваться как стоимость, когда утраченная информация не подлежит возмещению. Кроме того, при копировании информации, составляющей интеллектуальную собственности ее стоимость может быть уменьшена или сведена к нулю. Страхователь может быть не в состоянии самостоятельно компенсировать утраченную стоимость интеллектуальной собственности.

6.3.4.3 Вред репутации

Репутация является важным бизнес-активом для большинства организаций, и нанесение вреда репутации может быть катастрофическим. Для страхователя важно восстановить свою репутацию, если она была потеряна в результате инцидента ИБ. У страхователя должен быть соответствующий план реагирования на данный инцидент, подтверждающий его озабоченность и приверженность оперативному разрешению инцидента, который показывает, что страхователь контролирует ситуацию. Страховщики могут оказать поддержку в оплате услуг консультантов по связям с общественностью, чтобы помочь смягчить нанесенный вред репутации.

6.3.4.4 Расходы на оповещение клиентов и сотрудников

Инцидент ИБ может быть связан с информацией о клиентах или сотрудниках и потенциально повлиять на их защищенность. Если речь идет о персональных данных, то вполне возможно, что субъекты персональных данных, а также регулирующие органы могут потребовать ответа на вопрос о масштабах инцидента ИБ и мерах, предпринятых для минимизации причиненного вреда. В случае такого инцидента ИБ страхователь может понести расходы, связанные с необходимостью уведомления пострадавших лиц о том, что их персональные данные были подвержены атакам. Эти расходы могут включать в себя стоимость создания и поддержания деятельности специального центра обработки вызовов клиентов для обработки звонков от уведомленных субъектов.

6.3.4.5 Расходы на защиту клиентов и сотрудников

При наступлении инцидента ИБ, приведшем к утрате персональных данных клиентов и сотрудников, данные лица подвергаются повышенной опасности, вызванной мошеннической деятельностью (кража персональных данных, вымогательство). Расходы могут быть понесены в связи с тем, что страхователю, для снижения уровня подверженности риску, необходимо предоставить услуги по мониторингу кредитных операций или операций с персональными данными в течение определенного периода времени. Понесенные расходы могут также включать юридические, почтовые и рекламные расходы, если существует требование нормативных правовых актов уведомлять физических лиц о инциденте ИБ, включая расходы на кредитный мониторинг и поддержку средств массовой информации в области связей с общественностью.

6.3.4.6 Расходы на оплату услуг специалистов по реагированию на инциденты

Инцидент ИБ может вызвать сложные проблемы адекватного реагирования на его последствия, которые могут повлечь за собой расходы, связанные с привлечением специалистов или соответствующей команды для оказания помощи страхователю. Например, инцидент ИБ может быть связан с национальными и/или международными требованиями, которые требуют специальных знаний для определения эффективных способов реагирования и учета специальных требований нормативных правовых актов. Другим примером может быть использование страхователем услуг специалистов по кризисному взаимодействию для консультирования по вопросам взаимодействия со СМИ и общественностью, а также по вопросам составления планов кризисного взаимодействия и уведомления пострадавших и заинтересованных сторон. Иногда, в случае инцидента ИБ, с целью отражения атаки, остановки системного кризиса и его расследования могут потребоваться специальные ресурсы, которые могут включать специальную круглосуточную горячую линию по инцидентам ИБ и связанного с ней кол-центра для обработки звонков от уведомленных лиц, специалистов по ИТ-криминалистике.

6.3.4.7 Операционные расходы на управление инцидентами

Страхователь может понести затраты по реагированию на инциденты и сдерживания воздействия на деловые процессы организации. Например, перенаправление штатных экспертов на работу в составе группы быстрого реагирования, сверхурочные расходы, оперативные расходы на восстановление систем, сетей или данных.

6.3.4.8 Расходы на персонал

Наступление инцидента ИБ может привести к затратам на персонал. Например, на оплату сверхурочных часов, увеличение штатного состава, на компенсацию морального вреда личной репутации персонала.

6.3.5 Покрытие расходов, связанных с вымогательством

Вымогательство включает в себя попытки злоумышленника получить деньги путем угроз нанесения ущерба, ограничения использования каких-либо технологий страхователем или раскрытием информации, скопированной или похищенной у страхователя. Примерами подобного вымогательства могут являться:

- шифрование информации страхователя с помощью вредоносного программного обеспечения (ПО);
- угрозы совершения или совершение хакерской атаки, атаки типа «отказ в обслуживании» или внедрение вредоносного ПО в информационные системы страхователя;
- несанкционированное удаление, распространение, разглашение или использование информации, хранящейся в информационных системах страхователя;
- повреждение, разрушение или несанкционированное изменение конфигурации информационных систем страхователя;
- требование выкупа для расшифрования информации.

6.3.6 Расходы на прерывание деловых процессов организации

Прерывание производства и других деловых процессов организации, которое случилось в результате инцидента ИБ влечет за собой потерю дохода, упущенную выгоду или увеличение операционных расходов. Дальнейшие прерывание производства может включать снижение операционной эффективности и результативности, несоблюдение сроков и задержку поставок клиентам.

6.3.7 Штрафы и пени, связанные с нарушением законодательства

Инцидент ИБ может привести к тому, что страхователь подвергается:

- административной ответственности;
- штрафов, накладываемых регулирующим органом по результатам проведения расследования;
- прочим штрафам, прописанным в нормативных правовых актах.

6.3.8 Штрафы, связанные с нарушением договорных обязательств

Инцидент ИБ может привести к неисполнению страхователем договорных обязательств, что, в свою очередь может привести к наложению договорных штрафов со стороны других организаций.

6.3.9 Вред информационным системам

Инцидент ИБ может привести к затратам на ремонт или восстановление информационных систем, баз данных и программных приложений, которые не покрываются существующими страховыми полисами страховщика, например, где они специально исключены.

6.4 Риски поставщика

Инцидент ИБ, затрагивающий страхователя, может также произойти у поставщика или другой сторонней организации, предоставляющей товары или выполняющей услуги для страхователя. Такой инцидент ИБ может привести к потере данных или нарушить работу одной или нескольких служб, предоставляемых страхователю. Страхователь должен получить подтверждение того, что расходы, связанные с инцидентами ИБ у поставщика или другой сторонней организации, заключившей договор на поставку товаров или оказание услуг, будут возмещены либо через собственные страховые соглашения третьей стороны, либо страховым полисом страхователя.

В результате инцидента ИБ страхователь может понести расходы на расследование, на судебную защиту и возмещение вреда своему поставщику или другой подрядной сторонней организации.

С другой стороны, инцидент ИБ у страхователя может повлиять на деятельность клиентов или других внешних субъектов, в результате чего убытки, понесенные этими внешними субъектами, могут привести к претензиям или финансовым обязательствам страховщика.

6.5 Неявно выраженное покрытие рисков информационной безопасности в других страховых полисах

Некоторые потенциальные последствия инцидентов ИБ также могут быть отражены в существующих страховых полисах страхователя, в случае, если инциденты ИБ не исключены в качестве оговорки. Примером могут являться инциденты, приводящие к пожару или взрыву. Обычно такие инциденты описываются в полисах страхования материальных активов организации. Страхователь должен учитывать потенциальное покрытие, а также исключения рисков ИБ в существующих полисах.

6.6 Поставщики, продавцы и консультанты по реагированию на инциденты

Страхователь должен развивать и поддерживать отношения с поставщиками, продавцами и консультантами, чтобы подготовиться к инциденту ИБ и повысить свою способность своевременно и адекватно реагировать на инциденты ИБ. Эти отношения должны регулярно оцениваться и пересматриваться в рамках мероприятий по обеспечению непрерывности бизнеса страхователя. Эти услуги могут быть доступны, как в качестве услуги от страховщика, так и быть получены страхователем самостоятельно.

6.7 Исключения в полисе страхования рисков информационной безопасности

Полис страхования рисков ИБ не может покрыть все виды убытков. Поэтому необходимо, чтобы страхователь понимал, какие риски исключены из данного документа. Перечень исключений может содержать следующие элементы:

- физические повреждения кого-либо из сотрудников организации или третьих лиц, полученные в результате инцидента ИБ;
- терроризм: вред, вызванный хакерскими группировками, которые классифицируются как террористические организации в некоторых странах или международными организациями;
- военные действия и другие враждебные действия на государственном уровне, связанные с состоянием государства и уровнем разрушительного воздействия, независимо от наличия факта объявления войны;
- последствия утраты интеллектуальной собственности: например, патентов, авторских прав или коммерческой тайны;
- кража или утрата конфиденциальной информации, не принадлежащей страхователю;
- репутационный вред.

Страхователь должен быть уведомлен об исключенных типах покрытия рисков ИБ.

6.8 Пределы суммы покрытия

Потенциальные последствия для бизнеса и убытки, которые могут быть понесены страхователем, должны быть рассмотрены и уточнены, чтобы тщательно определить и рассмотреть объем покрытия и оценить стоимость полиса страхования рисков ИБ. Стоимость полиса страхования рисков ИБ может варьироваться в зависимости от финансовых показателей страхователя, отрасли, операций и подверженности риску ИБ. Примером может являться объем персональных данных, хранящихся у страхователя.

К полисам страхования рисков ИБ может применяться сверхнормативная сумма или франшиза, которая представляет собой сумму денег, которую страхователь должен заплатить, прежде чем можно будет предъявить иск по полису страхования рисков ИБ. Может быть совокупный лимит либо на полис целиком, либо на каждое событие в течение года. Размер и характер превышения или франшизы должны быть согласованы во время подготовки полиса страхования рисков ИБ. Полисы также могут включать период ожидания в несколько дней до того, как начинает применяться покрытие прерывания деловых процессов. Помимо прочего, продолжительность покрытия прерывания деловых процессов может быть ограничена. Большинство полисов покрывают доход, потерянный в результате наступления инцидента ИБ только в течение определенного периода времени.

Чтобы помочь в оценке потенциальных потерь, которые позволили бы определить надлежащий объем покрытия для покупки, можно обратиться за советом к исследовательским организациям, регулярно публикующим отраслевую информацию о стоимости финансовых потерь в результате случившихся инцидентов ИБ по всему миру.

7 Оценка рисков информационной безопасности, поддерживающая андеррайтинг

7.1 Обзор

Процесс андеррайтинга обычно включает в себя ряд подготовительных мероприятий, которые помогают определить, следует ли принимать риски ИБ страхователя и определить адекватную цену для покрытия рисков ИБ. Эти мероприятия включают в себя:

- правовые и организационные меры по обеспечению защиты конфиденциальности сведений о хозяйственной деятельности, в том числе и о системе защиты информации потенциального страхователя;
- сбор информации о методах защиты информации страхователя;
- оценку рисков ИБ страхователя;
- оценку операционных рисков;
- определение целесообразности страхования рисков ИБ страхователя;
- создание полиса страхования рисков ИБ и определение ее цены.

7.2 Сбор информации

Для проведения процесса андеррайтинга страховщик определяет необходимые данные и информацию о страхователе. Перечень необходимых данных может включать в себя, но не ограничиваться нижеуказанным:

- понимание миссии бизнеса страхователя;
- выявление ключевых заинтересованных сторон, включая клиентов и деловых партнеров;
- перечень сохраняемой и обрабатываемой информации;
- перечень информационных систем;
- сведения об аутсорсинговых договоренностях;
- сведения о СМИБ;
- перечень и описание применяемых мер обеспечения ИБ;
- записи о случившихся ранее инцидентах, в том числе и инцидентов ИБ;
- дополнительные гарантии состояния СМИБ, такие как аудиторские отчеты, акты проверок и результаты последующих действий.

Собираемая информация должна быть полной, актуальной, достоверной и защищена должным образом.

Страховщик может запрашивать регулярное обновление информации с определенной периодичностью. Страховщик на законных основаниях может запрашивать дополнительную информацию о рисках ИБ страхователя у третьих лиц, провайдеров, поставщиков услуг по оценке рисков.

Глубина такого сбора информации зависит от суммы и объема желаемого страхового покрытия, которое обычно относится к масштабам бизнеса страхователя. Страховщик решает самостоятельно, следует ли предоставлять такую дополнительную информацию страхователю.

7.3 Оценка рисков информационной безопасности

7.3.1 Обзор

Страховщик оценивает риски ИБ страхователя с целью определить, следует ли страховать его риски ИБ и определения адекватной цены за желаемое покрытие. При оценке риска рассматривается как подверженность страхователя риску ИБ, так и состояние действующих мер обеспечения ИБ.

7.3.2 Оценка неотъемлемых рисков информационной безопасности

Страховщик определяет типовой уровень риска страхователя на основе знания отраслевых секторов, иногда такой риск называется неотъемлемым риском с учетом следующих факторов:

- отрасли промышленности;
- масштаба организации;
- типа предпринимательской деятельности;
- объема и типа хранимой и используемой информации;
- зависимости от систем с внешним управлением или управлением сторонними организациями;
- страны, в которой ведется предпринимательская деятельность;
- перечня нормативных правовых актов, субъектом которых является организация.

Если страхователь относится к субъектам критической информационной инфраструктуры, то считается что он подвержен более высокому риску, в том числе и риску ИБ.

7.3.3 Оценка системы менеджмента информационной безопасности

Страховщик оценивает уровень защиты информации страхователя и защищенности его активов, а также способность противостоять атакам. Оценка страховщика может учитывать технологию, особенности бизнес-процесса, персонал, а также ссылаться на рекомендуемый перечень контролей. Рекомендуемый перечень контролей приведен в ГОСТ Р ИСО/МЭК 27002, который включает в себя следующее:

- наличие, содержание и непротиворечивость политик ИБ;
- организация защиты информации — определение и распределение отдельных ролей и обязанностей по обеспечению ИБ, для предотвращения конфликта интересов и несанкционированных действий;
- ответственность персонала — обязанности, учитываемые при управлении жизненным циклом работы сотрудников, подрядчиков и временного персонала;
- управление активами, в том числе информационными. Информационные активы должны быть учтены с учетом их владельцев, а также лиц, ответственных за обеспечение защиты активов, в том числе информационных;
- контроль доступа — ограничение доступа к информации и средствам обработки информации;
- применение криптографии — использование средств шифрования, криптографической аутентификации и контроля целостности, таких как цифровые подписи и коды аутентификации сообщений, а также управление криптографическими ключами;
- обеспечение физической безопасности и защиты от природных угроз — перечень средств контроля физического доступа и средств контроля рабочих процедур для защиты помещений, офисов, зон доставки или погрузки от несанкционированного доступа;
- обеспечение безопасности производственной деятельности — перечень процедур и обязанностей, защита от вредоносных программ, резервное копирование, ведение журнала и мониторинг, контроль используемого ПО, управление техническими уязвимостями и координация аудита информационных систем;
- обеспечение безопасности обмена информацией — управление ИБ, информационных сетей и процессов передачи и обработки информации;
- приобретение, разработка и обслуживание систем — требования к защите информации, информационных систем, безопасность процессов разработки и поддержания в готовности информационных систем, а также их тестирование;
- отношения с поставщиками — обеспечение защиты информации в отношениях с поставщиками и управление предоставлением услуг поставщикам;
- управление ИБ — управление инцидентами ИБ и улучшениями системы реагирования на инциденты ИБ;
- аспекты защиты информации в менеджменте непрерывности бизнеса — непрерывность и избыточность мер по обеспечению защиты информации;
- соответствие юридическим и договорным требованиям по обеспечению ИБ;
- соответствие требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти.

7.3.4 Уроки, извлеченные из случившихся ранее инцидентов

В тех случаях, когда компания понесла существенные убытки, в том числе и от инцидентов ИБ в прошлом, требуется повышенный уровень понимания шагов, предпринимаемых страхователем для уменьшения будущих убытков. Эта проверка может включать оценку финансового состояния страхователя (баланс, отчет о прибылях и убытках и отчет о движении денежных средств). Для минимизации будущих потерь до принятия решения о страховании может потребоваться принятие определенных новых мер обеспечения ИБ или усиление существующих.

8 Система менеджмента информационной безопасности в страховании рисков

8.1 Обзор

ГОСТ Р ИСО/МЭК 27001 предоставляет организациям структурированный подход по внедрению системы менеджмента информационной безопасности (СМИБ), предназначенной для создания, внедрения, поддержания и постоянного развития комплекса мер обеспечения ИБ. Эффективная СМИБ позволяет организации:

- выявлять, анализировать и устранять риски ИБ;
- постоянно защищать организацию от угроз ИБ;
- анализировать и совершенствовать СМИБ, чтобы оперативно реагировать на динамику изменения угроз ИБ, появление новых уязвимостей и последствий для бизнеса.

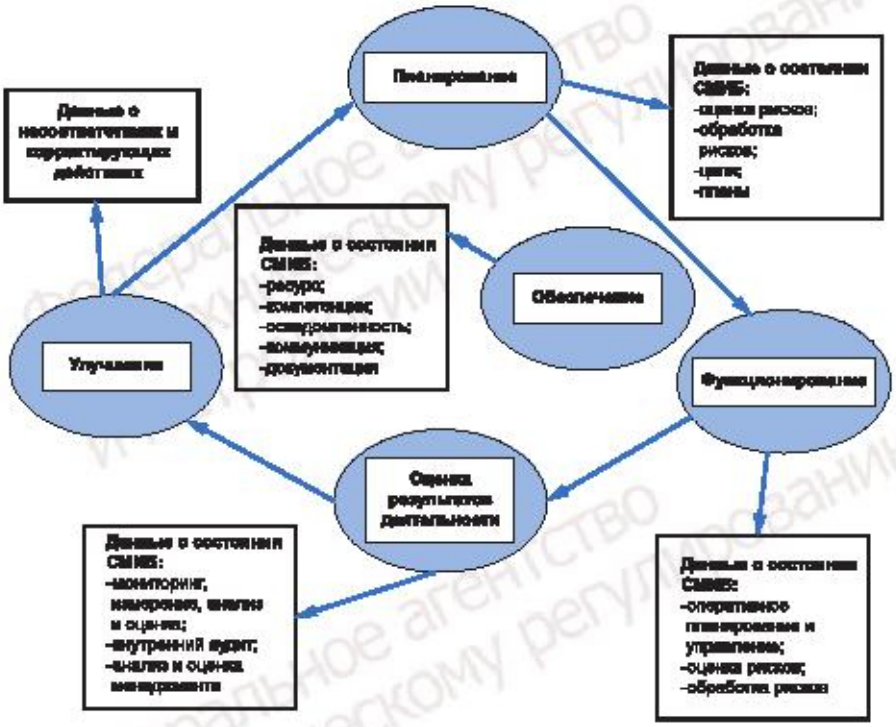
СМИБ может предоставить страхователю и страховщику данные, информацию и документацию, которые могут быть использованы при формировании полиса страхования рисков ИБ, его обновлении, а также в течение всего срока его действия. Поскольку страхование рисков ИБ является вариантом распределения рисков, предоставление страховщику информации о СМИБ может способствовать разработке обоснованного варианта полиса страхования рисков ИБ.

8.2 Система менеджмента информационной безопасности как источник исходных данных для страхования

8.2.1 Система менеджмента информационной безопасности

СМИБ, которая создается, внедряется, поддерживается и постоянно совершенствуется в соответствии с ГОСТ Р ИСО/МЭК 27001, может служить источником исходных данных, могущих быть использованными при обосновании условий полиса страхования рисков ИБ, условий его обновления.

Страхователь должен собирать, систематизировать и сопоставлять результаты функционирования СМИБ (например, на основе ГОСТ Р ИСО/МЭК 27004 и ГОСТ Р ИСО/МЭК 27005) и представлять страховщику необходимые данные). В приложении А приводится перечень документов, которые могут служить в качестве исходных данных для принятия решения о страховании рисков ИБ. Структура исходных данных, источником которых является СМИБ приведена на рисунке 1.



Примечание — Фигуры на рисунке 1 относятся к соответствующим пунктам, приведенным в ГОСТ Р ИСО/МЭК 27001.

Рисунок 1 — Структура исходных данных, источником которых является СМИБ

8.2.2 Планирование

При планировании, страхователь определяет риски, которыми необходимо управлять, чтобы:

- СМИБ могла достичь намеченных результатов;
- предотвращать или уменьшать нежелательные эффекты;
- обеспечить постоянное улучшение результата.

Страхователь определяет и реализует процесс оценки и обработки рисков ИБ, а также принимает меры по хранению соответствующей документированной информации.

В планах управления рисками ИБ должны содержаться меры, которые страхователь считает необходимыми для их снижения. Такой контроль документируется в документе «Заявление о применимости» (SoA) страхователя.

8.2.3 Обеспечение

Лица, выполняющие работу по контролю деятельности страхователя и руководящие или участвующие в создании, внедрении, поддержании и постоянном совершенствовании СМИБ, должны знать:

- политики ИБ;
- их вклад в обеспечение эффективности СМИБ;
- последствия несоответствия требованиям СМИБ.

Информация об обучении отдельных лиц страхователя может быть затребована страховщиком.

Страхователь определяет необходимость внутренних и внешних коммуникаций, относящихся к СМИБ, в том числе:

- содержание коммуникации;
- время коммуникации;
- субъектов коммуникации;
- сотрудников, осуществляющих управление коммуникацией;
- процессы, запускающие коммуникации.

Страхователь должен применять вышеуказанные правила, чтобы определить, как лучше всего взаимодействовать со страховщиком.

При внедрении, применении и обслуживании СМИБ страхователь разрабатывает следующую документацию:

- согласно требованиям, указанным в ГОСТ Р ИСО/МЭК 27001;
- определенную страхователем как необходимую для эффективного функционирования СМИБ.

Примечание — Примеры такой дополнительной документации см. в ГОСТ Р ИСО/МЭК 27003.

Документация, созданная выше, может быть затребована страховщиком.

8.2.4 Функционирование

При реализации требований СМИБ страхователю необходимо:

- планировать, внедрять и контролировать процессы, необходимые для выполнения требований по обеспечению ИБ;
- хранить записи, записи, изложения фактов и иную информацию, которая существенна с точки зрения обеспечения уверенности в том, что определенные процессы были выполнены в соответствии с планом;
- контролировать запланированные изменения и анализировать последствия непреднамеренных изменений, принимая меры для смягчения любых неблагоприятных последствий, если это необходимо;
- гарантировать, что внешние процессы определены и контролируются;
- проводить оценку рисков ИБ через запланированные промежутки времени или когда предполагаются или происходят существенные изменения с учетом критериев, установленных на этапе планирования, и сохранять документированную информацию о результатах оценки этих рисков;
- реализовать план обработки рисков ИБ и сохранить документированную информацию о результатах обработки этих рисков.

Страхователь может предоставлять страховщику документацию, подготовленную на этом этапе.

8.2.5 Оценка результатов деятельности

Оценка результатов деятельности может служить источником сведений об эффективности применения мер обеспечения ИБ (как технических, так и иных), что позволит страховщику сопоставлять и представлять информацию об эффективности и результативности СМИБ в целом. Данные могут быть собраны со следующих источников:

- от самих органов управления СМИБ;
- средств измерений;

- результатов аудитов ИБ, в том числе внутренних;
- с помощью метрик, представленных в ГОСТ Р ИСО/МЭК 27004;
- средств мониторинга, обзора и оценки мер обеспечения ИБ или процессов, которые они поддерживают.

Внутренние аудиты информационной безопасности, мер обеспечения ИБ или СМИБ в целом могут быть использованы для сбора дополнительных данных об эффективности и действенности СМИБ и обеспечить бизнес-контекст для полученных данных. При необходимости для сбора этих данных можно также использовать внешние аудиты.

Страхователь должен проводить плановые проверки СМИБ с определенными интервалами, чтобы обеспечить ее постоянную готовность, адекватность и эффективность.

Данные, собранные на этапе оценки рисков ИБ, могут быть использованы для выявления несоответствий и областей, требующих постоянного улучшения, а также могут быть отражены в качестве документированной информации, которая в свою очередь может быть использована в качестве доказательства результатов мониторинга и измерений. Данные результаты впоследствии могут быть переданы страховщику.

При оценке результатов деятельности по управлению ИБ могут быть выявлены новые риски ИБ или изменения ранее выявленных рисков ИБ, которые могут быть задокументированы и предоставлены страховщику.

8.2.6 Улучшение

Реагирование на выявленные несоответствия и принятые меры позволяют управлять рисками ИБ. Процесс управления рисками ИБ должен быть документирован.

Страхователь также может задокументировать шаги, предпринятые для совершенствования, адекватности и обеспечения эффективности СМИБ. Страхователь может предоставить страховщику документацию по усовершенствованию СМИБ.

8.2.7 Обмен информацией о рисках информационной безопасности и мерах по контролю

Поскольку страхование рисков ИБ является одним из способов управления названными рисками, то целесообразно чтобы страхователь регулярно информировал страховщика об уровне ИБ и соответствии ее деловым целям.

Периодичность и содержание такого обмена должны быть согласованы между страхователем и страховщиком.

В процессе страхования рисков информационной безопасности страхователь и страховщик обмениваются информацией с целью:

- демонстрации страхователем своих усилий по защите от угроз ИБ;
- определения рисков ИБ, подлежащих разделению со страховщиком;
- оценки страховщиком принимаемого им риска, отражения его в полисе страхования рисков ИБ и определения цены страхового полиса, включая применимые франшизы или исключения.

Информация о рисках ИБ должна быть полной и актуальной. Невыполнение этого условия может привести к аннулированию страхового полиса со стороны страховщика. Предоставление ложной информации может привести к аннулированию страхового полиса со стороны страховщика и к судебному иску против страхователя или лиц, причастных к предоставлению этой ложной информации.

Страхователь должен иметь утвержденную процедуру реагирования на запросы страховщика по предоставлению информации при формировании страхового полиса и его обновлении. Запросы могут поступать периодически в течение всего срока действия, а также при возникновении инцидента ИБ. Страхователь должен предоставлять информацию страховщику в согласованном формате.

Страхователь должен предоставлять страховщику по его запросу полную документацию, касающуюся принятых организационных и технических мер обеспечения ИБ и деятельности по управлению рисками ИБ.

Такие запросы могут включать в себя документацию по СМИБ, отчеты о внутреннем или внешнем аудитах, а также результаты проверок, проведения сертификаций, а также политики, процедуры и руководящие принципы по обеспечению ИБ.

Страхователь должен предусмотреть условия предоставления информации о договорных отношениях с партнерами для передачи ее страховым компаниям либо заключить дополнительные соглашения о соблюдении конфиденциальности такой информации.

8.3 Выполнение обязательств по договору страхования рисков информационной безопасности

Страховщик может потребовать определенного исходного уровня ИБ в качестве предварительного условия страхового покрытия. Такие условия отражаются в договоре страхования информационной безопасности, и страхователь должен соблюдать эти условия в течение всего срока действия договора.

Кроме того, при обработке заявки на страхование рисков ИБ страховщику следует запросить у страхователя информацию о принятых организационных и технических мерах по защите информации, которые должны поддерживаться в течение всего срока действия договора страхования.

Сведения о СМИБ могут служить исходными данными для страхователя при заполнении опросных листов и выполнении обязательств, изложенных в страховом полисе.

Приложение А
(справочное)

Перечень документов системы менеджмента информационной безопасности для обмена информацией со страховщиком

В данном приложении приводится перечень документации, относящейся к СМИБ страхователя, которые могут использоваться в качестве свидетельства при оценке рисков информационной безопасности страхователя. Эти документы могут использоваться для этой цели в случае, если область действия СМИБ охватывает область страхования информационных рисков.

Перечень документов разделяется на две категории:

- категория 1. Документы, определенные в [2] (см. таблицу А.1);
- категория 2. Документы, которые определил страхователь как важные.

См. [2] (пункт 7.5.1, перечисления а) и б)) для формулирования требований.

Страховщик и страхователь могут определить перечень документации, требуемый для передачи страховщику (см. раздел 8).

Таблица А.1 — Документация, требуемая согласно [2]

Пункт [2]	Информация
4.3	Определение области действия системы менеджмента информационной безопасности
5.2	Политика информационной безопасности
6.1.2	Оценка рисков информационной безопасности
6.1.3	Ведомость применимости
6.1.3	Процесс обработки рисков информационной безопасности
6.2	Цели в области информационной безопасности
7.2	Доказательства компетентности персонала
7.5	Доказательства эффективности СМИБ
8.1	Доказательства эффективности процессов информационной безопасности
8.2	Результаты оценки рисков информационной безопасности
8.3	Результаты обработки рисков информационной безопасности
9.1	Результаты мониторинга и измерений результатов деятельности по информационной безопасности
9.2	Результаты проведения внутреннего аудита
9.3	Результаты анализа системы менеджмента
10.1	Результаты анализа характера несоответствий и любых последующих предпринятых действий
10.1	Результаты любого корректирующего действия

Документы, которые страхователь определил как важные, могут включать:

- политики, руководства и процедуры защиты информации;
- документы о внутренних ролях и ответственности страхователя;
- планы и записи программ обучения;
- документы по управлению процессами, осуществляемыми на внешнем подряде;
- записи о процессах реагирования на инциденты.

Библиография

[1] Закон РФ от 27 ноября 1992 г. № 4015-1«Об организации страхового дела в Российской Федерации» (ред. от 28 ноября 2018 г.)

[2] ИСО/МЭК 27001:2013 Информационные технологии. Методы обеспечения защиты. Системы обеспечения информационной безопасности. Требования
(Information technology — Security techniques — Information security management systems — Requirements)

УДК 006.34:004 ОКС 35.030

Ключевые слова: система менеджмента информационной безопасности, информационная безопасность, страхование рисков информационной безопасности, угроза информационной безопасности, страховщик, страхователь, атака, инцидент информационной безопасности

Редактор *В.Н. Шмельков*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.05.2021. Подписано в печать 03.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru