ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УКАЗАНИЕ

«26» июня 2023 г. № 6466-У

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 75425
от "02" октября 2023 г.

О требованиях к организации оператором автоматизированной информационной системы страхования системы управления рисками

Настоящее Указание на основании подпункта 8 пункта 7 статьи 33^{10} Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации» устанавливает требования к организации оператором автоматизированной информационной системы страхования системы управления рисками.

1. Оператор автоматизированной информационной системы страхования, указанной в пункте 1 статьи 33^{10} Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации» (далее – АИС страхования), должен организовать систему управления рисками, включающую в себя, в частности, следующие элементы:

процедуры управления рисками, содержащие комплекс применяемых оператором АИС страхования действий, направленных на минимизацию отрицательных последствий случаев фактической реализации рисков (далее – риск-событие);

классификатор рисков, используемый в системе управления рисками, включающий в себя риски, которые должны учитываться в рамках процедуры управления рисками (далее – классификатор рисков);

базу риск-событий, содержащую характеристики риск-события (описание риск-события, обстоятельства, повлекшие наступление риск-события, сведения о мероприятиях, направленных на минимизацию последствий наступления риск-события, статус исполнения таких мероприятий);

контрольные показатели уровня рисков, содержащихся в классификаторе рисков, с указанием их предельных значений.

2. Оператор АИС страхования в рамках организации системы управления рисками должен определить во внутренних документах меры, направленные на снижение операционных и иных рисков, реализация которых оказывает влияние на операционную надежность оператора АИС страхования, требования к которой установлены Банком России в соответствии с подпунктом 5 пункта 7 статьи 33^{10} Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации», включая:

риск реализации информационных угроз, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, используемых оператором АИС страхования, а также несоответствием указанных процессов деятельности оператора АИС страхования (далее – риск информационной безопасности);

риск отказа и (или) нарушения функционирования применяемых оператором АИС страхования информационных систем и (или) несоответствия их функциональных возможностей и характеристик потребностям оператора АИС страхования.

3. Оператор АИС страхования в рамках организации системы управления рисками должен определить во внутренних документах классификатор рисков, содержащий классификацию рисков в зависимости от источников риска, типов риск-событий, направлений деятельности, в том числе в разрезе составляющих их процессов, видов потерь от реализации риска, мер, направленных на минимизацию или предотвращение рисков, и мероприятий по обеспечению непрерывности деятельности оператора АИС страхования.

Оператор АИС страхования должен поддерживать классификатор рисков в актуальном состоянии с учетом изменений осуществляемых операций и (или) действующих процессов оператора АИС страхования.

4. Оператор АИС страхования в целях управления риском информационной безопасности должен определить во внутренних документах порядок управления указанным риском, включающий в себя:

определение политики информационной безопасности;

выявление и идентификацию риска информационной безопасности, а также его оценку;

участие единоличного исполнительного органа и (или) специализированного комитета (специализированных комитетов) оператора АИС страхования (если это предусмотрено внутренними документами) в решении вопросов управления риском информационной безопасности;

распределение функций и ответственности единоличного исполнительного органа и работников оператора АИС страхования, в том числе исключающее конфликт их интересов в рамках организационной структуры обеспечения информационной безопасности;

организацию ресурсного (кадрового и финансового) обеспечения, в том числе установление требований к квалификации работников оператора АИС страхования, ответственных за обеспечение защиты информации;

выявление событий риска информационной безопасности, в том числе рассмотрение обращений пользователей АИС страхования, связанных с нарушением защиты информации;

мониторинг риска информационной безопасности;

планирование, разработку, реализацию, контроль и совершенствование комплекса мероприятий, направленных на уменьшение негативного влияния риска информационной безопасности, а также комплекса мероприятий, направленных на обеспечение соответствия фактических значений контрольных показателей уровня риска информационной безопасности значениям, принятым оператором АИС страхования;

обеспечение защиты от угроз безопасности информации, в том числе обеспечение защиты информации, управление риском информационной безопасности при передаче третьим лицам (внешним подрядчикам, контрагентам) отдельных функций оператора АИС страхования и (или) при использовании внешних информационных систем в рамках реализации функций оператора АИС страхования, управление риском несанкционированного доступа к АИС страхования, осуществляемого работником оператора АИС страхования или третьим лицом, обладающим

полномочиями по доступу к прикладному программному обеспечению автоматизированных систем и приложениям, используемым оператором АИС страхования, предотвращение не контролируемого оператором АИС страхования распространения информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в АИС страхования, а также обеспечение операционной надежности в условиях реализации информационных угроз;

реагирование на выявленные события риска информационной безопасности оператора АИС страхования в случае реализации таких событий.

5. Оператор АИС страхования в целях контроля за уровнем рисков должен определить во внутренних документах на плановый годовой период контрольные показатели уровня рисков, а также установить целевые значения этих показателей.

6. Оператор АИС страхования в рамках организации системы управления рисками должен определить структурное подразделение, ответственное за организацию управления рисками.

7. Оператор АИС страхования в рамках организации системы управления рисками должен определить независимое от подразделения оператора АИС страхования, ответственного за организацию управления рисками, подразделение или лицо, уполномоченное осуществлять оценку эффективности выполнения процедур управления рисками оператора АИС страхования (в том числе на предмет их полноты и корректности), и предоставлять результаты указанной оценки в виде отчета на рассмотрение совету директоров и коллегиальному исполнительному органу оператора АИС страхования в срок, установленный во внутренних документах оператора АИС страхования.

8. Настоящее Указание вступает в силу по истечении 10 дней после дня его официального опубликования.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина