Об утверждении методики оценки рисков информационной безопасности, включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 23 ноября 2020 года № 111. Зарегистрировано в Министерстве юстиции Республики Казахстан 27 ноября 2020 года № 21686.

Настоящее постановление вводится в действие с 1 января 2021 года.

В соответствии с подпунктом 2) части первой статьи 13-6 Закона Республики Казахстан от 4 июля 2003 года "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую Методику оценки рисков информационной безопасности , включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности.

2. Управлению кибербезопасности в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Агентства Республики Казахстан по регулированию и развитию финансового рынка после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент сведений об исполнении мероприятия, предусмотренного подпунктом 2) настоящего пункта.

3. Контроль за исполнением настоящего постановления возложить на курирующего заместителя Председателя Агентства Республики Казахстан по регулированию и развитию финансового рынка.

4. Настоящее постановление вводится в действие с 1 января 2021 года и подлежит официальному опубликованию.

Председатель Агентства
Республики Казахстан по регулированию и
развитию финансового рынка *М. Абылкасымова*

Утверждена постановлением
Правления Агентства
Республики Казахстан по

регулированию и развитию
финансового рынка
от 23 ноября 2020 года № 111

Методика оценки рисков информационной безопасности, включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности

Глава 1. Общие положения

1. Настоящая Методика оценки рисков информационной безопасности, включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности (далее - Методика), разработана в соответствии с Законом Республики Казахстан от 4 июля 2003 года "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" и применяется в целях организации процесса оценки рисков информационной безопасности в финансовых организациях и филиалах банков - нерезидентов Республики Казахстан, филиалах страховых (перестраховочных) организаций - нерезидентов Республики Казахстан, филиалах страховых брокеров - нерезидентов Республики Казахстан (далее – финансовые организации), к которым предъявляются требования по проведению оценки рисков информационной безопасности, для определения приоритетов и оптимизации ресурсов, задействованных при обработке рисков информационной безопасности в финансовых организациях.

2. В Методике используются следующие понятия:

1) бизнес-владелец информационного актива – владелец основного бизнес-процесса , для обеспечения жизненного цикла которого используется информационный актив;

2) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

3) риск информационной безопасности – вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности информационных активов;

4) уровень риска информационной безопасности - комбинация вероятности события и его последствий;

5) уровень существенности убытков от нарушения информационной безопасности – уровень убытков от нарушения информационной безопасности в финансовой организации, превышение которого по отдельному информационному активу не приемлемо для финансовой организации;

6) критичный информационный актив – информационный актив, определяемый в соответствии с постановлением Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 "Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики

Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах", зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 16772.

Сноска. Пункт 2 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 29.04.2022 № 30 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

3. Для оценки рисков информационной безопасности финансовой организацией проводятся следующие мероприятия:

1) формирование перечня критичных информационных активов;

2) оценка рисков информационной безопасности для критичных информационных активов.

Глава 2. Формирование перечня критичных информационных активов

4. В целях формирования и последующей актуализации перечня критичных информационных активов финансовые организации обеспечивают реализацию следующих процессов:

1) анализ бизнес-процессов, входящих в область действия системы управления информационной безопасностью финансовой организации;

2) определение потенциальных убытков от нарушения свойств информационной безопасности (конфиденциальности, целостности и доступности) информационных активов;

3) формирование и последующая актуализация перечня критичных информационных активов.

5. Анализ бизнес-процессов, входящих в область действия системы управления информационной безопасностью финансовой организации, осуществляется подразделениями-владельцами бизнес-процессов финансовой организации под руководством подразделения по управлению рисками финансовой организации с целью идентификации информационных активов, необходимых для функционирования бизнес-процессов. Виды идентифицируемых информационных активов определяются по перечню видов информационных активов согласно приложению 1 к Методике.

Для идентификации информационных активов по решению подразделения-владельца бизнес-процесса финансовой организации привлекается подразделение по информационным технологиям финансовой организации.

6. По каждому идентифицированному информационному активу финансовая организация определяет следующие виды потенциальных убытков от нарушения информационной безопасности:

1) убытки от нарушения конфиденциальности информационного актива;

2) убытки от нарушения целостности информационного актива;

3) убытки от нарушения доступности информационного актива.

Убытки определяются бизнес-владельцами информационных активов под руководством подразделения по управлению рисками финансовой организации.

7. Для оценки потенциальных убытков от нарушения информационной безопасности информационных активов финансовая организация обеспечивает участие в оценке убытков сотрудников, обладающих знаниями:

1) внутренних документов финансовой организации, регламентирующих профессиональную деятельность, соответствующую бизнес-процессам, в которых используются информационные активы;

2) бизнес-процессов, в которых используются информационные активы, а также процессов работы с информационными активами;

3) факторов, влияющих на размер потенциальных убытков, указанных в пункте 8 Методики.

8. Определение потенциальных убытков от нарушения конфиденциальности, целостности и доступности информационного актива финансовой организацией осуществляется с учетом следующих факторов:

1) степень влияния нарушения на жизненный цикл бизнес-процессов в финансовой организации;

2) степень влияния нарушения на деловую репутацию финансовой организации;

3) объем возможных финансовых потерь финансовой организации;

4) последствия от возможного нарушения требований законодательства Республики Казахстан, в том числе нормативных правовых актов уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее – уполномоченный орган), и (или) договорных обязательств финансовой организации;

5) объем критичной защищаемой информации, обрабатываемой информационным активом.

9. В целях осуществления классификации информационных активов подразделение по управлению рисками финансовой организации устанавливает уровень существенности убытков от нарушения информационной безопасности. Уровень существенности убытков от нарушения информационной безопасности определяется в соответствии с риск-аппетитом для операционных рисков в финансовой организации или риск-аппетитом для рисков информационной безопасности при его наличии в финансовой организации.

10. Перечень критичных информационных активов формируется и актуализируется рабочей группой под руководством подразделения по управлению рисками финансовой организации. В перечень критичных информационных активов включаются

информационные активы, убытки от нарушения свойств которых превышают установленный уровень существенности убытков от нарушения информационной безопасности. Для каждого критичного информационного актива указывается его вид и тип в соответствии с Перечнем видов информационных активов согласно приложению 1 к Методике, убытки от нарушения свойств (конфиденциальности, целостности и (или) доступности), а также бизнес-владелец информационного актива.

Глава 3. Оценка рисков информационной безопасности для критичных информационных активов

11. В целях осуществления оценки рисков информационной безопасности для критичных информационных активов финансовые организации обеспечивают реализацию следующих процессов:

1) идентификация угроз информационной безопасности критичным информационным активам;

2) идентификация источников угроз информационной безопасности, релевантных для критичных информационных активов;

3) идентификация уязвимостей критичных информационных активов;

4) идентификация существующих мер управления рисками информационной безопасности;

5) оценка вероятности реализации угроз информационной безопасности критичным информационным активам источниками угроз информационной безопасности;

6) оценка уровня рисков информационной безопасности.

12. Идентификация угроз информационной безопасности критичным информационным активам осуществляется подразделением по информационной безопасности финансовой организации. Для каждого критичного информационного актива анализируются угрозы информационной безопасности, в том числе указанные в Перечне угроз информационной безопасности информационным активам согласно приложению 2 к Методике.

13. Идентификация источников угроз информационной безопасности, релевантных для критичных информационных активов, осуществляется подразделением по информационной безопасности финансовой организации на основании перечня критичных информационных активов, указанного в пункте 10 Методики, и угроз информационной безопасности критичным информационным активам, идентифицированных в соответствии с пунктом 12 Методики. Для каждой идентифицированной угрозы информационной безопасности критичным информационным активам анализируются релевантные источники угроз информационной безопасности с учетом источников угроз информационной безопасности, указанных в Перечне типовых источников угроз информационной безопасности согласно приложению 3 к Методике.

14. Идентификация уязвимостей критичных информационных активов осуществляется подразделением по информационной безопасности финансовой организации на основании перечня критичных информационных активов, указанного в пункте 10 Методики, с учетом следующей информации о (об):

1) конструкции информационного актива;

2) физическом расположении информационного актива;

3) известных ошибках в программном коде;

4) ошибках в конфигурации;

5) недостатках процесса эксплуатации информационного актива.

15. Идентификация существующих мер управления рисками информационной безопасности для критичных информационных активов осуществляется подразделением по информационной безопасности финансовой организации на основании перечня критичных информационных активов, указанного в пункте 10 Методики, с учетом информации об организационных и технических мероприятиях, направленных на исправление существующих недостатков в процессе обеспечения информационной безопасности критичных информационных активов либо последствий ее нарушения.

16. Оценка вероятности реализации угроз информационной безопасности критичным информационным активам источниками угроз информационной безопасности осуществляется подразделением по информационной безопасности финансовой организации для всех релевантных для критичного информационного актива комбинаций источника угрозы информационной безопасности, угрозы информационной безопасности и уязвимости, с учетом следующей информации:

1) данные о расположении источника угрозы информационной безопасности относительно соответствующих критичных информационных активов (внутренний или внешний). Для внутренних источников угроз информационной безопасности учитывается количество пользователей актива, для внешних источников угроз информационной безопасности – наличие возможного доступа извне периметра защиты;

2) данные об уровне доступа источника угрозы информационной безопасности;

3) статистические данные о частоте реализации угрозы информационной безопасности критичному информационному активу в прошлом;

4) информация о сложности реализации угрозы информационной безопасности критичному информационному активу;

5) данные о наличии у рассматриваемых критичных информационных активов защитных мер.

17. При привлечении к оценке вероятности реализации угрозы информационной безопасности критичным информационным активам источниками угроз информационной безопасности нескольких экспертов и получении разных оценок

итоговая, обобщенная оценка принимается равной оценке, определяющей наибольшую вероятность.

18. Оценка уровня рисков информационной безопасности проводится на основании сопоставления оценок вероятности реализации угрозы информационной безопасности критичным информационным активам источниками угроз информационной безопасности и оценок соответствующих потенциальных убытков от нарушения конфиденциальности, целостности или доступности критичного информационного актива.

Глава 4. Ранжирование финансовых организаций по степени подверженности рискам информационной безопасности

19. Ранжирование финансовых организаций по степени подверженности рискам информационной безопасности осуществляется уполномоченным органом по следующим показателям:

1) показатель потенциальных убытков, который определяется как общая сумма потенциальных убытков от нарушения конфиденциальности, целостности и доступности всех критичных информационных активов финансовой организации;

2) показатель доли критичных информационных активов, который определяется как соотношение общей суммы убытков от нарушения конфиденциальности, целостности и доступности всех критичных информационных активов к собственному капиталу банка или уставному капиталу организации, осуществляющей отдельные виды банковских операций.

20. Информация для осуществления ранжирования предоставляется финансовыми организациями по запросу уполномоченного органа.

21. Для показателя потенциальных убытков ранжирование осуществляется от максимального к минимальному.

22. Для показателя доли критичных информационных активов ранжирование осуществляется от минимального к максимальному.

Приложение 1 к Методике
оценки рисков информационной
безопасности,
включая порядок ранжирования
финансовых организаций по
степени подверженности рискам
информационной безопасности

Перечень видов информационных активов

Вид актива	Тип
Индивидуальное устройство обработки информации (компьютер, планшет, ноутбук, смартфон)	Аппаратный
Носитель информации	Аппаратный

Периферийное компьютерное оборудование	Аппаратный
Сервер	Аппаратный
Сетевое оборудование	Аппаратный
Аппаратура телефонии	Аппаратный
Физический канал связи	Аппаратный
База данных	Программный
Виртуальный канал связи	Программный
Система виртуализации	Программный
Операционная система	Программный
Программное обеспечение аппаратных средств	Программный
Прикладное программное обеспечение	Программный
Программное обеспечение телефонии	Программный

Приложение 2 к Методике
оценки рисков информационной
безопасности,
включая порядок ранжирования
финансовых организаций по
степени подверженности рискам
информационной безопасности

Перечень угроз информационной безопасности информационным активам

Тип актива	Угроза информационной безопасности	Влияние
Аппаратный	Физическое хищение	Конфиденциальность, доступность
Аппаратный	Несанкционированный физический доступ	Конфиденциальность, целостность, доступность
Аппаратный	Физическое разрушение	Доступность
Программный	Удаление	Доступность
Программный	Исполнение несанкционированного кода	Конфиденциальность, целостность, доступность
Программный	Программная ошибка	Конфиденциальность, целостность, доступность
Программный	Ошибка конфигурации	Конфиденциальность, целостность, доступность

Приложение 3 к Методике
оценки рисков информационной
безопасности,
включая порядок ранжирования
финансовых организаций по
степени подверженности рискам
информационной безопасности

Перечень типовых источников угроз информационной безопасности

Источник угрозы информационной безопасности	Расположение	Уровень доступа

Хакеры	Внешнее	Низкий
Пользователь	Внутреннее	Средний
Привилегированный пользователь	Внутреннее	Высокий