Об утверждении требований к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89. Зарегистрировано в Министерстве юстиции Республики Казахстан 23 сентября 2020 года № 21251.

Примечание ИЗПИ!

Настоящее постановление вводится в действие с 1 января 2021 года.

В соответствии с подпунктом 3) 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 прилагаемые Требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение 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*

Приложение к постановлению
Правления Агентства
Республики Казахстан

по регулированию и развитию
финансового рынка
от 21 сентября 2020 года № 89

Требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности

Глава 1. Общие положения

1. Настоящие Требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности (далее – Требования) разработаны в соответствии с Законом Республики Казахстан от 4 июля 2003 года "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" и устанавливают требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности (далее – работники) финансовых организаций Республики Казахстан и филиалов банков-нерезидентов Республики Казахстан, филиалов страховых (перестраховочных) организаций-нерезидентов Республики Казахстан, филиалов страховых брокеров-нерезидентов Республики Казахстан (далее – организации) независимо от форм собственности.

Сноска. Пункт 1 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 17.02.2021 № 34 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

2. В Требованиях используются следующие понятия:

1) информационная безопасность - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

2) домен - совокупность знаний в отдельной предметной области;

3) компетенция - результат усвоения информации, полученный в процессе обучения и личного опыта; совокупность знаний, теории и практики, относящихся к сфере обучения или работы; компонент квалификации, который подвергается оценке.

В Требованиях применяются термины и определения в соответствии с Межгосударственным стандартом ГОСТ ISO/IEC 17024-2014 "Оценка соответствия. Общие требования к органам, осуществляющим сертификацию персонала" (далее – Стандарт).

Сноска. Пункт 2 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 20.10.2022 № 71 (вводится в

действие по истечении десяти календарных дней после дня его первого официального опубликования).

3. Требования основываются на принципах:

1) разграничения функциональных обязанностей по типовым должностям;

2) направленности на знания и навыки в области информационных технологий и информационной безопасности, включая кибербезопасность;

3) независимости от требований, предъявляемых производителями программного обеспечения и аппаратного оборудования к работникам;

4) баланса теоретических знаний и практических навыков, профессиональных компетенций, предъявляемых к типовым должностям;

5) использования типовых доменов.

4. Типовые должности в организации:

1) специалист - работник подразделения информационной безопасности, в функциональные обязанности которого входит обеспечение информационной безопасности организации;

2) руководитель - работник подразделения информационной безопасности, в функциональные обязанности которого входит организация деятельности подразделения информационной безопасности;

3) ответственный работник - работник, выполняющий одновременно функциональные обязанности специалиста и руководителя.

5. Разделение компетенций на домены предназначено для:

1) баланса возможностей и специфики организации по обеспечению информационной безопасности;

2) формирования требования с учетом квалификации, компетенции работников и особенностей бизнес-процессов организации;

3) расширения требований за счет создания новых доменов.

Глава 2. Состав доменов

6. Домены содержат минимально необходимый перечень компетенций, которые по усмотрению организации дополняются, расширяются при необходимости.

7. Состав типовых доменов:

1) базовый;

2) правовой;

3) организационный;

4) программно-аппаратный;

5) телекоммуникационный;

6) методы и средства обеспечения информационной безопасности;

7) управление рисками информационной безопасности;

8) управление инцидентами информационной безопасности.

8. Состав домена "базовый" - терминология и требования системы управления информационной безопасностью.

9. Состав домена "правовой":

1) национальные, международные стандарты в области информационной безопасности;

2) законодательные и нормативные правовые акты в области информационной безопасности;

3) методические документы уполномоченных органов по защите информации.

10. Состав домена "организационный":

1) основы, цели, принципы управленческой деятельности;

2) основы информационно-аналитической деятельности;

3) основные организационные меры и мероприятия по защите информации.

11. Состав домена "программно-аппаратный":

1) общие принципы функционирования программно-аппаратных средств;

2) принципы построения, работы программно-аппаратных комплексов защиты информации;

3) порядок устранения неисправностей программно-аппаратных средств защиты информации.

12. Состав домена "телекоммуникационный":

1) принципы построения информационных систем и сетей телекоммуникаций;

2) источники угроз информационной безопасности в сетях телекоммуникаций и меры по их предотвращению;

3) назначение, цели, возможности эксплуатируемых средств защиты информации на объектах телекоммуникаций;

4) методы и средства защиты информации от несанкционированного доступа в сетях телекоммуникаций.

13. Состав домена "методы и средства информационной безопасности":

1) организационные аспекты информационной безопасности;

2) управление информационными активами;

3) управление доступом.

14. Состав домена "управление рисками информационной безопасности":

1) процесс управления рисками информационной безопасности:

2) основные критерии менеджмента рисков;

3) оценка рисков информационной безопасности;

4) обработка, принятие рисков информационной безопасности.

15. Состав домена "управление инцидентами информационной безопасности":

1) цели и задачи группы реагирования на инциденты;

2) план управления инцидентами.

Глава 3. Требования к знаниям и опыту работы

16. Обязательным для всех должностей является домен "базовый".

17. К специалисту дополнительно к домену "базовому" предъявляются требования о наличии компетенций не менее, чем по одному из доменов.

18. К специалисту предъявляется требование о соответствии одному из критериев:

1) наличие среднего специального или высшего образования по одному из доменов;

2) прохождение обучения по одному или более доменам;

3) опыт работы по одному и более доменам не менее двух лет;

4) наличие сертификата, подтверждающего знания и опыт по одному или более доменам, выданного в соответствии с требованиями Стандарта или Международного стандарта ISO/IEC 17024:2012 "Conformity assessment - general requirements for bodies operating certification of persons" (Комфомити ассесмент – дженерал реквайрментс фор бодиес операtинг сертификэйшн оф персонс) (Оценка соответствия. Общие требования к органам, осуществляющим сертификацию персонала) (далее – Международный стандарт).

Сноска. Пункт 18 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 20.10.2022 № 71 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

19. Требования к руководителю включают в себя минимально необходимый перечень компетенций в соответствии с возложенными на подразделение информационной безопасности задачами.

20. К руководителю предъявляются требования о наличии высшего образования и опыта работы не менее трех лет по одному из доменов.

21. Оценка компетенций руководителя осуществляется в соответствии с внутренними документами организации. Решение о его соответствии оформляется документально.

21-1. Не менее пяти процентов работников подразделения информационной безопасности в организации, указанных в пункте 4 Требований, подтверждают соответствие критериям подпункта 4) пункта 18 Требований.

Сноска. Требования дополнены пунктом 21-1 в соответствии с постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 20.10.2022 № 71 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Глава 4. Требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности

22. Специалисты и руководители не реже одного раза в 3 (три) года повышают квалификацию путем прохождения обучения или сертификации по темам, указанным в доменах.

23. Подтверждением повышения квалификации специалистов и руководителей, ответственных за обеспечение информационной безопасности, является наличие документов о прохождении обучения и (или) сертификата, выданного в соответствии со Стандартом или Международным стандартом.

Сноска. Пункт 23 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 20.10.2022 № 71 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).