ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ТӨТЕНШЕ ЖАҒДАЙЛАР МИНИСТРЛІГІ

БҰЙРЫҚ

_____

Нұр-Сұлтан қаласы

МИНИСТЕРСТВО ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ РЕСПУБЛИКИ КАЗАХСТАН

ПРИКАЗ

№_____

город Нур-Султан

Приказ № 152 от 31.03.2021г.

Об утверждении Политики информационной безопасности органов гражданской защиты

В соответствии с пунктом 32 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 **ПРИКАЗЫВАЮ:**

1. Утвердить прилагаемую Политику информационной безопасности органов гражданской защиты.

2. В целях обеспечения информационной безопасности и технической защиты государственных секретов в Министерстве по чрезвычайным ситуациям Республики Казахстан (далее - Министерство), возложить функции по обеспечению:

1) технической защиты государственных секретов на Управление специальной работы Министерства;

2) сохранности информации служебного пользования на Департамент документационного обеспечения и развития государственного языка Министерства;

3) целостности информационно-коммуникационных систем и отдельных информационных систем на Департамент информатизации, цифровизации и связи Министерства.

3. Руководителям структурных и территориальных подразделений, подведомственных организаций Министерства в повседневной деятельности руководствоваться настоящей Политикой информационной безопасности.

4. Контроль за исполнением настоящего приказа возложить на первого вице-министра по чрезвычайным ситуациям Республики Казахстан Кульшимбаева И.Д.

5. Настоящий приказ вступает в силу со дня его подписания.

Министр
генерал-майор **Ю. Ильин**

Утверждено
приказом Министра
по чрезвычайным ситуациям
Республики Казахстан
от « » 2021 года
№

Политика информационной безопасности
в органах гражданской защиты

Глава 1. Общие положения

1. Политика информационной безопасности органов гражданской защиты Республики Казахстан (далее – Политика) содержит комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов и включает в себя требования в адрес пользователей информационных систем (сервисов) органов гражданской защиты (далее – ОГЗ), поставщиков и технических служб.

2. Настоящая Политика разработана в соответствии с постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

3. Организация (построение) и обеспечение эффективного функционирования системы защиты информации в центральном аппарате Министерства по чрезвычайным ситуациям (далее –- МЧС) возлагается на Департамент информатизации, цифровизации и связи МЧС, являющийся структурным подразделением, занимающийся вопросами создания, сопровождения и развития объектов информатизации.

В территориальных подразделениях и подведомственных учреждениях, ведомствах и подведомственных организациях МЧС приказом руководителя назначается специалист ответственный за обеспечение информационной безопасности, который подчиняется первому руководителю, либо иному лицу в составе руководства ОГЗ, курирующего вопросы обеспечения информационной безопасности, непосредственно подчиненный первому руководителю (далее – Ответственный за информационную безопасность).

Глава 2. Цели и задачи системы управления информационной безопасности

4. Основной целью обеспечения информационной безопасности в ОГЗ является предотвращение потери конфиденциальности, целостности и доступности защищаемых активов, в том числе:

1) недопущение нанесения материального, физического, морального или иного ущерба в результате информационной деятельности;

2) предотвращение остановки основных бизнес-процессов;

3) предотвращение уничтожения имущества и ценностей;

4) предотвращение разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации;

5) предотвращение нарушения работы технических средств обеспечения производственной деятельности, включая и средства информатизации.

5. Для достижения вышеуказанных целей должны быть решены, в том числе следующие задачи:

1) обеспечение активного участия руководства в управлении информационной безопасностью;

2) повышение осведомленности сотрудников в области рисков, связанных с информационными ресурсами;

3) распределение ответственности и обязанностей сотрудников по обеспечению информационной безопасности;

4) разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам;

5) регистрация действий пользователей в системных журналах при использовании сетевых ресурсов;

6) контроль корректности действий пользователей систем путем анализа содержимого этих журналов;

7) защита от вмешательства посторонних лиц в процесс функционирования информационных систем и общесистемного программного обеспечения;

8) контроль целостности используемых программных средств, среды исполнения программ и ее восстановление в случае нарушения, а также защиты систем от внедрения вредоносных кодов;

9) защита информации с ограниченным распространением, персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

10) аутентификация пользователей информационных систем и ресурсов;

11) своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

12) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц;

13) ликвидация последствий нарушения информационной безопасности;

14) разработка и внедрения правил и инструкции по обеспечению информационной безопасности, контроля исполнения соответствующих требований сотрудниками;

15) реализация мероприятий по оценке и управлению информационными рисками;

16) совершенствование системы управления информационной безопасностью.

Глава 3. Основные принципы обеспечения информационной безопасности

6. Обеспечение информационной безопасности в ОГЗ основывается на следующих принципах:

1) соблюдение требований законодательства Республики Казахстан;

2) соответствие международным и национальным стандартам в области информационной безопасности, действующим на территории Республики Казахстан;

3) постоянный и всесторонний анализ информационного пространства с целью выявления уязвимостей активов;

4) адекватная оценка степени влияния выявленных проблем на цели ОГЗ;

5) комплексное использование методов и средств защиты компьютерных систем, перекрывающих все существенные каналы реализации угроз и не содержащих слабых мест на стыках отдельных ее компонентов;

6) эффективная реализация принятых защитных мер;

7) обеспечение соответствующего уровня защищенности электронных информационных ресурсов, программного обеспечения, информационных систем и поддерживающей их информационно-коммуникационной инфраструктуры в соответствии с классом объекта информатизации;

8) применение рекомендаций стандартов в области информационно-коммуникационных технологий и информационной безопасности на всех этапах жизненного цикла объектов информатизации;

9) приверженность к непрерывному совершенствованию системы менеджмента информационной безопасности.

Глава 4. Субъекты информационных отношений

7. Субъектами правоотношений при использовании информации и обеспечении информационной безопасности являются:

1) ОГЗ;

2) должностные лица и сотрудники ОГЗ;

3) пользователи и поставщики информации в соответствии с возложенными на них функциями;

4) юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются средствами и системами, а также информация на бумажных носителях;

5) другие юридические и физические лица, задействованные в процессе создания, сопровождения, модификации и развития средств и систем организаций (разработчики информационных систем и других прикладных программ, обслуживающий и технический персонал).

Глава 5. Организация системы управления информационной безопасностью

8. Ответственность за общее состояние системы управления информационной безопасности (далее - СУИБ) несет первый руководитель.

9. Мероприятия по организации системы управления информационной безопасностью возлагаются на Ответственного за информационную безопасность, который отвечает за:

1) общую организацию СУИБ, координацию и контроль деятельности всех подразделений ОГЗ в части создания и поддержания системы обеспечения информационной безопасности;

2) методологическую поддержку процесса обеспечения информационной безопасности;

3) выбор, внедрение и применение методов, средств и механизмов контроля, управления и обеспечения информационной безопасности;

4) обеспечение внедрения, надлежащего функционирования и мониторинга программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности;

5) организацию и проведение мероприятий по поддержанию осведомленности персонала в вопросах информационной безопасности;

6) мониторинг состояния системы управления информационной безопасностью;

7) учет и обработку событий и инцидентов, связанных с нарушением состояния информационной безопасности;

8) информирование руководства о состоянии СУИБ.

Глава 6. Меры по защите информации и средств ее обработки

10. Информация и средства обработки информации должны быть расположены и защищены так, чтобы уменьшить риск от воздействий окружающей среды и возможности неавторизованного доступа. Для защиты активов ОГЗ, применяются:

организационные меры защиты - меры административного и процедурного характера, регламентирующие процессы функционирования систем обработки данных, использование их ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с объектом информатизации, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации;

физические меры защиты - основаны на применении специализированных механических, электро- или электронно-механических устройств и сооружений, предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам объекта информатизации и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов объекта информатизации (пломбы, наклейки, паспорта, перечни оборудования и программного обеспечения);

технические (аппаратно-программные) меры защиты - основаны на использовании различных электронных устройств и специальных программ, входящих в том числе в состав объекта информатизации и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

Глава 7. Особенности обеспечения физической безопасности активов, связанных со средствами обработки информации

11. В зданиях и помещениях ОГЗ необходимо организовать круглосуточное дежурство сотрудников службы охраны и (или) установить тревожную сигнализацию с выводом на пульт специализированной службы охраны.

12. Доступ в помещения ОГЗ, не предназначенные для постоянного нахождения в них сотрудников и (или) посетителей, ограничивается и контролируется. При организации гостевого доступа в такие помещения обеспечивается регистрация посетителей ОГЗ, с выдачей пропусков, внешне отличающихся от пропусков работников ОГЗ, а также обеспечивается технический и организационный контроль над перемещением посетителей.

13. Требования к создаваемой или модернизируемой локальной сети определяются в техническом задании на локальную сеть. При проектировании кабельной системы локальной сети необходимо пользоваться нормами СН РК 3.02-17-2011 «Структурированные кабельные сети. Нормы проектирования».

14. При проектировании создается и при эксплуатации поддерживается в актуальном состоянии документированная схема локальной сети.

15. Все элементы кабельной системы подлежат маркировке. Все кабельные соединения регистрируются в журнале учета кабельных соединений, допускается ведение журнала в электронном виде.

16. Неиспользуемые порты телекоммуникационного оборудования от кабельной системы локальной сети физически или программно отключаются, с соответствующей отметкой в журнале учета кабельных соединений.

17. Оборудование и техническое оснащение серверного помещения должны соответствовать требованиям параграфа 8 главы 3 постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» и стандартам Республики Казахстан и максимально приближены к международным стандартам, в том числе EIA/TIA-569.

Глава 8. Обеспечение безопасности периметра защиты информационной инфраструктуры

18. Необходимо определить периметр защиты информационной инфраструктуры (далее – Периметр). Подразделением информационной безопасности составляется, утверждается и поддерживается в актуальном состоянии: схема Периметра, информационных потоков, выходящих за Периметр, и перечень администраторов средств обеспечения безопасности периметра.

19. Телекоммуникационные соединения, за исключением соединений с городской телефонной сетью, выходящие за периметр защиты ОГЗ, а также соединения между территориально удаленными сетями и устройствами ОГЗ, необходимо шифровать вне зависимости от типа соединения. При использовании беспроводных соединений шифрование необходимо производить дополнительными методами, отличными от

методов шифрования, предоставляемых протоколом беспроводного соединения при наличии технической возможности.

20. Ввод телекоммуникационных сетей (Интернет, ЕТС ГО, IP-VPN) в здание обеспечивается через пограничный шлюз (прокси-сервер, маршрутизатор, межсетевой экран), расположенный в серверном помещении. Все сети телекоммуникаций подключаются в режиме «bridge» к пограничному шлюзу, отдельно к каждому, внешнему и внутреннему контуру локальной сети.

21. Допускается подключение не более одной точки доступа к сети Интернет в отдельно стоящее здание.

22. Не допускается прямое подключение сети телекоммуникаций (Интернет, ЕТС ГО, IP-VPN) к коммутаторам локальной сети;

23. Коммутация структурированных кабельных систем должна проходить через сетевое оборудование, установленное в серверном помещении.

24. При превышении длины магистралей, устанавливаются этажные коммутационные центры, размещенные на этажах здания или местах концентрации большого количества пользователей. При этом, активное сетевое оборудование должно размещаться в телекоммуникационных шкафах (помещениях), с обеспечением защиты от несанкционированного доступа.

25. Для ограничения доступа на Периметре устанавливаются межсетевые экраны. Правила доступа и конфигурация, установленные на межсетевых экранах, разрешают только те соединения, которые необходимы для функционирования бизнес-процессов. Такие правила доступа, а также вносимые в них изменения согласовываются с ответственным сотрудником по информационной безопасности ЦА.

26. Для выявления и отражения атак на Периметр, устанавливаются средства обнаружения и предотвращения вторжений. Их конфигурация согласовывается с ответственным сотрудником по информационной безопасности ЦА.

27. Необходимо предусматривать механизмы предотвращения атак типа «отказ в обслуживании». Такие механизмы используют как штатные механизмы систем обеспечения безопасности Периметра, так и дополнительные меры (договоры с провайдерами телекоммуникационных услуг, установка специализированных систем, имеющих соответствующий функционал по защите от атак данного типа).

28. Доступ к внешним информационным активам ОГЗ, извне (внешние информационные ресурсы) осуществляется извне через сетевой периметр демилитаризированной зоны, отделенной от внутренних информационных активов межсетевым экраном. Обмен данными с информационными активами ОГЗ, доступ к которым необходим извне, осуществляется с использованием механизмов, обеспечивающих безопасность при построении подобного обмена, такими как межсетевые экраны, сегментирование сети и отделение внутренней сети ОГЗ от внешней среды с помощью демилитаризованной зоны.

29. Для обеспечения безопасности и централизации доступа пользователей к ресурсам сети Интернет необходимо устанавливать соответствующие шлюзы, позволяющие осуществлять:

1) очистку трафика от вирусов;
2) блокировку ресурсов Интернет, содержащих деструктивные функции;
3) очистку почтового трафика от спама.

Необходимо чтобы конфигурация средств обеспечения безопасности периметра соответствовала рекомендациям производителей и регулярно пересматривалась, с учетом выявления новых угроз и уязвимостей, но не реже одного раза в год.

Глава 9. Обеспечение защиты информационных систем

30. Для каждой информационной системы определяется ее владелец по следующим принципам:

1) информационная система закрепляется за подразделением, являющимся владельцем основного бизнес-процесса, автоматизируемого данной информационной системой;

2) инфраструктурные информационные системы закрепляются за подразделением информатизации, цифровизации и связи;

31. В обязанности владельца информационной системы входит поддержание информационной системы в состоянии, отвечающем требованиям обеспечения информационной безопасности, принятым.

32. Необходимо чтобы процесс разработки (приобретения) информационной системы, а также проведения доработок в информационной системе, состоял из следующих этапов:

1) инициирование процесса - инициатором разработки (приобретения) или доработки информационной системы, автоматизирующей конкретный бизнес-процесс, является владелец бизнес-процесса;

2) разработка технического задания - служба информационных технологий совместно с владельцем информационной системы создает техническое задание на разработку (закуп, доработку) информационной системы и определяет необходимые трудозатраты;

3) согласование и утверждение - техническое задание согласовывается со службой информационной безопасности, и выносится на рассмотрение уполномоченного органа, определяющего целесообразность и очередность разработки (приобретения) или доработки;

4) разработка (приобретение, доработка) - служба информационных технологий разрабатывает (приобретает, дорабатывает) информационную систему;

5) тестирование - владелец бизнес-процесса, владелец информационной системы и иные заинтересованные подразделения тестируют информационную систему по специально разработанной методике тестирования на предмет соответствия функциональным требованиям и техническому заданию;

6) опытная эксплуатация - на основании акта об успешном тестировании, в том числе, на соответствие системы существующим в ОГЗ требованиям информационной безопасности, служба информационных технологий переводит информационную систему в промышленную среду, ограничивая эксплуатацию информационной системы лимитом по количеству конечных пользователей, масштабом или областью применения информационной системы. Владелец бизнес-процесса и владелец информационной системы продолжают ее тестирование на предмет наличия ошибок, которые не выявлены в тестовом режиме;

7) промышленная эксплуатация - на основании акта об успешном прохождении опытной эксплуатации информационная система переводится в промышленную эксплуатацию.

33. Запрещается разработка и доработка информационных систем в среде промышленной эксплуатации.

Среды разработки, тестирования и промышленной эксплуатации необходимо отделять друг от друга таким образом, чтобы изменения, внесенные в любой из этих сред, не влияли на информационную систему, расположенную в другой среде.

Среды разработки, тестирования и промышленной эксплуатации максимально приближены друг к другу в части программного и аппаратного обеспечения.

Необходимо чтобы промышленные данные, в случае нахождения в средах разработки и тестирования обезличивались или маскировались.

34. Необходимо чтобы работники службы информационных технологий, осуществляющие разработку (доработку) информационных систем, не имели полномочий на перенос информационной системы в тестовую и промышленную среды, а также не имели административный доступ к информационной системе в промышленной среде.

35. Перед вводом в опытную эксплуатацию информационной системы в ней необходимо изменять настройки безопасности в соответствии с правилами обеспечения информационной безопасности. Как минимум необходимо изменять пароли, используемые при тестировании, отключать все неиспользуемые встроенные учетные записи, а также удалять все тестовые учетные записи. Также составляются и утверждаются перечни администраторов информационных систем.

36. В процессе обеспечения контроля над использованием привилегированных учетных записей необходимо использовать как минимум один из перечисленных способов:

1) разделение пароля к привилегированной учетной записи между двумя работниками ОГЗ;

2) установка разового сложного пароля к привилегированной учетной записи для каждого сеанса, его хранением у руководителя службы информационных технологий и выдачи только на период проведения работ с последующей заменой на новый сразу по окончанию работ;

3) введение двойного контроля при исполнении функций администрирования информационных систем;

4) применение специальных программно-аппаратных средств контроля использования привилегированных учетных записей.

37. Обеспечивается резервное хранение критичных данных информационных систем, их важных файлов и настроек. Периодичность и порядок резервирования устанавливаются ОГЗ самостоятельно, в целях обеспечения непрерывности деятельности ОГЗ. Хранение резервных копий необходимо дублировать в помещении, территориально удаленном от основного серверного помещения.

38. ОГЗ самостоятельно принимает решение о способе восстановления работоспособности критичных информационных систем, аппаратном резервировании информационных систем (горячее или холодное резервирование, аппаратное или программное), с учётом требуемого времени доступности.

Глава 10. Управление обновлениями и уязвимостями

39. Информационные системы обеспечиваются технической поддержкой, в состав которой входят услуги по централизованному предоставлению обновлений соответствующей информационной системы. Допускается осуществление технической поддержки сотрудниками, если разработчик (вендор) прекратил официальную техническую поддержку, либо свернул свою деятельность. В этом случае необходимо рассмотреть вопрос о замене информационной системы.

40. Необходимо отслеживать выход обновлений информационных систем, публикации о выявленных уязвимостях в используемых ОГЗ информационных системах и определяет политику управления обновлениями для информационных систем.

41. Необходимо чтобы обновления информационной системы проходили испытания в тестовой среде до установки в промышленную среду.

Необходимо предпринять все возможные меры по устранению выявленных уязвимостей.

42. Обновления безопасности информационной системы, устраняющие критичные уязвимости, устанавливаются на информационную систему не позднее одного месяца со дня их публикации и распространения производителем. В случае невозможности установки обновлений в указанные сроки, связанные с функциональными особенностями информационной системы, для такой системы применяются компенсирующие меры снижения риска эксплуатации критичной уязвимости, с обоснованием эффективности этих мер.

43. Подразделение информационной безопасности проводит технический анализ (аудит) защищенности критичных информационных систем на наличие уязвимостей с использованием специализированного программного обеспечения. Аудит проводится не реже одного раза в год для каждой информационной системы как сотрудниками информационной безопасности, так и внешними специализированными компаниями. Результаты аудита формируются в виде отчета о состоянии информационной безопасности с указанием рекомендаций о необходимых корректирующих и превентивных действиях по устранению выявленных уязвимостей.

По окончании работ по устранению уязвимостей проводится повторный аудит информационной системы, подтверждающий устранение ранее выявленных уязвимостей.

Глава 11. Обеспечение защиты рабочих станций и мобильных устройств

44. Программное обеспечение рабочих станций лицензируется соответствующим образом, с соблюдением всех условий, определяющих обязательства и ответственность для сторон лицензионного договора.

45. Определяются минимальные требования по обеспечению информационной безопасности для используемого программного обеспечения.

Перед вводом программного обеспечения в эксплуатацию необходимо провести следующую экспертизу:

1) в службе информатизации и связи на предмет совместимости с остальным программным обеспечением;

2) в службе информационной безопасности на предмет соответствия программного обеспечения требованиям обеспечения информационной безопасности ОГЗ.

Установка и настройка программного обеспечения и оборудования производится работниками службы информатизации и связи.

46. Запрещено предоставление пользователям на рабочей станции прав локального администратора или аналогичных им за исключением случаев, когда такие права необходимы для функционирования программного обеспечения, автоматизирующего функции, исполняемые пользователем.

47. Допускается отдельным группам пользователей (например, работникам службы информационной безопасности, отвечающим за сопровождение технических средств безопасности) предоставление права самостоятельно устанавливать и настраивать программное обеспечение и оборудование. Этим группам пользователей допускается предоставление права локального администратора или аналогичные им.

48. В случае подключения мобильных устройств к информационным системам извне периметра защиты, на данных устройствах необходимо устанавливать специальное программное обеспечение, обеспечивающее защищенный доступ к информационным системам (шифрование канала связи, обеспечение двухфакторной аутентификации, дистанционное удаление данных).

49. При использовании для обработки информационных активов ОГЗ личных устройств работников ОГЗ, на данные устройства необходимо устанавливать специальное программное обеспечение, обеспечивающее разделение сред обработки личных данных и информационных активов.

Глава 12. Управление доступом в информационные системы

50. Доступ в информационные системы ОГЗ предоставляется в соответствии с Правилами разграничения прав доступа к электронным информационным системам, которые включают в себя:

1) процедура регистрации пользователей;

2) изменение и аннулирование прав доступа пользователей;

51. Создается и утверждается для каждой информационной системы, формализующую уровень полномочий работы в информационной системе на основе шаблонов (ролей).

52. Процесс создания матрицы доступа (далее - МД) включает в себя:

1) инициирование процесса – инициатором и разработчиком МД в информационных системах является владелец бизнес-процесса;

2) согласование – включает в себя согласование с заинтересованными подразделениями ОГЗ;

3) владелец информационной системы несет ответственность за:

соответствие уровня полномочий доступа для каждой роли в информационной системе, в соответствии с функциональными обязанностями пользователя;

распределение прав доступа пользователям информационной системы, с учетом минимальных и достаточных полномочий для выполнения возложенных на сотрудников должностных обязанностей;

исключение конфликта интереса в запрашиваемых ролях.

53. Внесение изменений и дополнений в роли пользователей и МД проходит те же этапы, что и процесс создания. Роли пользователей пересматриваются регулярно с периодичностью, определяемой руководством ОГЗ, но не реже одного раза в год для каждой информационной системы.

54. При изменении должности или функциональных обязанностей работника удаляются все имеющиеся права доступа и присваиваются новые, в соответствии с необходимым функционалом. При увольнении работника удаляются все его права доступа в информационные системы, не позднее дня увольнения. ОГЗ устанавливается порядок временной приостановки прав доступа в информационные системы, при длительном отсутствии работника.

55. Службой информационной безопасности создается процесс мониторинга регистрации пользователей и соответствие их прав доступа ролям в информационных системах, а также процесс контроля отключения прав доступа уволенных работников.

Глава 13. Обеспечение информационной безопасности при доступе третьих сторон

56. ОГЗ определяет требования по обеспечению информационной безопасности при доступе к информационным активам третьих сторон, не являющихся работниками ОГЗ, но в силу исполняемых обязанностей, нуждающихся в использовании информационных активов. К таковым относятся представители государственных органов Республики Казахстан, производящие проверку деятельности организации, дочерние организации, стажеры и практиканты, а также представители организаций и другие лица, оказывающие услуги организации на основании заключённых договоров.

57. Доступ третьих сторон к информационным активам ОГЗ предоставляется только на время и в объеме, необходимом для проведения соответствующих работ. Если третьей стороне в соответствии с ограничениями, наложенными законодательством Республики Казахстан, запрещено иметь доступ к части защищаемой информации, эта информация передается ей только в обезличенном или маскированном виде, не позволяющем восстановить защищаемые данные.

58. ОГЗ необходимо убедиться всеми доступными и не противоречащими законодательству Республики Казахстан способами (наличие публикаций в средствах массовой информации, государственных органов, рекомендательные письмами) в надежности третьей стороны, за исключением представителей государственных органов Республики Казахстан, производящие проверку деятельности ОГЗ.

59. В договорах, заключаемых с третьими сторонами, содержатся условия, предусматривающие ответственность за разглашение защищаемой информации, положение о конфиденциальности, а также ответственность за сбои в работе информационных систем и нарушения их безопасности, вызванные вмешательством третьей стороны. Допускается заключение с третьими сторонами отдельного

соглашения о конфиденциальности, содержащего указанные условия, а также срок действия такого соглашения.

60. ОГЗ необходимо удостовериться в полномочиях лиц, осуществляющих проверку деятельности ОГЗ или запрашивающих защищаемую информацию до предоставления им соответствующего доступа или информации.

В зависимости от оценки риска ОГЗ предусматривает организационные и программно-технические меры по контролю деятельности третьих сторон.

61. В случае передачи третьим сторонам части информационных активов ОГЗ (например, размещение серверных мощностей в сторонних ЦОД, использование облачных сервисов) ОГЗ предпринимает как минимум следующие меры обеспечения информационной безопасности:

1) отражение в договоре с третьей стороной ответственности за разглашение защищаемой информации и работоспособности информационных систем;

2) исключение возможности доступа третьей стороны к той части защищаемой информации, которая не может быть передана третьей стороне в соответствии с требованиями законодательства Республики Казахстан. При использовании облачных сервисов для этих целей необходимо применить метод хранения защищаемой информации в зашифрованном (токенизированном) виде с раскрытием информации на стороне ОГЗ.

Глава 14. Ведение аудита в информационных системах

62. Подразделениями информатизации, цифровизации и связи настраивается ведение аудита в информационных системах ОГЗ.

В аудите, как минимум, отражаются следующие события:

1) события подключений и входа/выхода в системе;
2) события модификации настроек безопасности;
3) события модификации групп пользователей и их полномочий;
4) события модификации учетных записей пользователей и их полномочий;
5) события, отражающие установку обновлений и (или) изменений в информационную систему;
6) события изменения параметров аудита;
7) события изменений системных параметров.

63. Формат аудита включает, как минимум, следующую информацию:

1) идентификатор (логин) пользователя, совершившего действие;
2) дата и время совершения действия;
3) имя рабочей станции пользователя и IP адрес, с которого совершено действие;
4) название объектов, с которыми проводилось действие;
5) тип/название совершенного действия (INSERT, UPDATE, DELETE);
6) результат действия (успех или неудача);
7) в случае изменения данных – содержимое изменяемого поля до изменения (при наличии технической возможности);
8) приложение, посредством которого осуществлен доступ.

64. Срок хранения аудита составляет не менее трех месяцев в оперативном доступе и не менее одного года в архивном доступе. Допускается агрегированное хранение

аудиторского следа нескольких информационных систем в специализированной информационной системе хранения, обработки и анализа событий.

65. Запрещается доступ на изменение данных аудита для всех пользователей. Администраторам информационных систем предоставляется доступ только на перенос журналов аудита в архив, при этом запрещается проведение редактирования содержимого архива.

66. Аудит ведется как на уровне операционных систем, приложения, так и на уровне СУБД информационной системы. При этом необходимо придерживаться принципа разумной достаточности: ни одно событие не должно произойти без записи в соответствующий журнал, но в целях экономии ресурсов информационных систем не следует дублировать информацию о данном действии в нескольких журналах.

Глава 15. Мониторинг событий информационной безопасности, управление инцидентами

67. ОГЗ определяет перечни событий информационной безопасности, подлежащих мониторингу, источников событий, периодичность, правила мониторинга и метод мониторинга:

1) ручной мониторинг – поиск необходимых событий информационной безопасности среди множества зарегистрированных событий в информационных системах;

2) полуавтоматический мониторинг – анализ событий информационной безопасности на основании автоматически сформированной выборки событий одного типа;

3) автоматический мониторинг – мониторинг с использованием специализированных систем анализа и корреляции событий информационной безопасности, позволяющих не только производить выборку событий по типу, но и автоматически оценивать их критичность.

68. В случае если имеется необходимость мониторинга отдельных источников событий информационной безопасности во внерабочее время, создается круглосуточная служба мониторинга.

69. Срок хранения информации о событиях информационной безопасности не менее трех месяцев в оперативном доступе и не менее одного года в архивном доступе.

70. Перечни событий информационной безопасности, подлежащих мониторингу, источников событий, периодичность, правила мониторинга и метод мониторинга пересматриваются не реже одного раза в год с учетом имеющейся статистики и эффективности мониторинга.

71. ОГЗ определяются основные критерии классификации события информационной безопасности как инцидента информационной безопасности.

72. ОГЗ определяется порядок информирования о произошедшем инциденте информационной безопасности руководящих работников и подразделений ОГЗ.

73. ОГЗ определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий.

74. ОГЗ проводит всесторонний анализ причин возникновения инцидента, его механизма и последствий.

75. Для инцидентов информационной безопасности, вероятность возникновения которых высока и отсутствует возможность ее снизить в ближайшем будущем, создаются отдельные документы, описывающие алгоритм обработки инцидента такого рода, типовых неотложных мер по локализации инцидента и его последствий, методов обработки инцидента.

76. На основании анализа инцидента подготавливается заключение, в котором отражается вся информация об инциденте, а также предложения по проведению корректирующих мер, в целях снижения вероятности и возможного ущерба от повторного инцидента.

77. ОГЗ ведет журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте, принятых мерах и предлагаемых корректирующих мерах. Допускается ведение журнала как на бумажном носителе, так и в электронном виде.

Глава 16. Проведение внутренних проверок состояния информационной безопасности

78. Внутренние проверки состояния информационной безопасности проводятся Ответственными за информационную безопасность в соответствии с планом, утверждаемым руководством или курирующим заместителям;

79. По результатам проверки составляется отчет, который подписывается руководителем проверки и утверждается (в случае необходимости) соответствующим уполномоченным лицом, определенным во внутренних нормативных документах. Отчет доводится до сведения проверяемого подразделения. Материалы проверки (выдержки из аудита, объяснительные пользователей, отчеты специальных систем анализа состояния информационной безопасности) предоставляются в случае обсуждения разногласий по выявленным недостаткам с сотрудниками проверяемого подразделения. При обнаружении в ходе проверки незначительных несоответствий требованиям обеспечения информационной безопасности или возможности возникновения таких несоответствий проверяющий отражает их в отчете и предлагает необходимые превентивные и (или) корректирующие меры.

80. В случае если при проверке обнаружены серьезные нарушения требований обеспечения информационной безопасности, попадающие под классификацию инцидента информационной безопасности, проверяющий инициирует обработку инцидента информационной безопасности, при этом в отчете отражается информация о выявленном инциденте.

81. Корректирующие и превентивные меры, предложенные в процессах обработки инцидентов и проверок состояния информационной безопасности, а также полученные в ходе иных процессов (например, оценки рисков), доводятся до подразделений, отвечающих за их реализацию.