ҚАЗАҚСТАН
РЕСПУБЛИКАСЫ ҰЛТТЫҚ
ЭКОНОМИКА МИНИСТРЛІГІ

«ҚАЗАҚСТАНДЫҚ
МЕМЛЕКЕТТІК-
ЖЕКЕ МЕНШІК ӘРІПТЕСТІК
ОРТАЛЫҒЫ» АКЦИОНЕРЛІК
ҚОҒАМЫ

РЕСПУБЛИКА КАЗАХСТАН
МИНИСТЕРСТВО
НАЦИОНАЛЬНОЙ
ЭКОНОМИКИ

АКЦИОНЕРНОЕ
ОБЩЕСТВО
«КАЗАХСТАНСКИЙ ЦЕНТР
ГОСУДАРСТВЕННО-
ЧАСТНОГО ПАРТНЕРСТВА»

KAZAKHSTAN PUBLIC-PRIVATE PARTNERSHIP CENTER

010000, Нұр-Сұлтан қаласы, Сол жағалау, Шұбар т.а., Темірқазық көшесі, 65, ҚСҚ 3, Экономика үйі ғимараты

Тел./факс: (7172) 70 17 24
(7172) 70 17 45

010000, г. Нур-Султан, Левый берег, ж.м. Чубары, ул. Темирказык, 65, ВП3, здание «Дом Экономики»

ВЫПИСКА
из протокола очного заседания Правления
АО «Казахстанский центр государственно-частного партнерства»

г. Нур-Султан *№30* *28 декабря 2021 года*

Местонахождение Правления АО «Казахстанский центр государственно-частного партнерства»: Республика Казахстан, 010000, г. Нур-Султан, район Есиль, ж.м. Чубары, ул. Темірказык, д. 65, ВП 3.

Время открытия и дата проведения: 28 декабря 2021 года

Кворум для принятия решения: имеется.

Форма заседания: очная (онлайн).

Место проведения: г. Нур-Султан, район Есиль, ж.м. Чубары, ул. Темірказык, д. 65, ВП 3.

По шестому вопросу повестки дня:

6. «Об утверждении Политики информационной безопасности АО «Казахстанский центр государственно-частного партнерства».

РЕШЕНИЕ:

Рассмотрев вопрос повестки дня и представленные материалы, в соответствии с подпунктом 4) пункта 73 Устава АО «Казахстанский центр государственного частного партнерства», подпунктом 3) пункта 30 Положения о Правлении АО «Казахстанский центр государственного частного партнерства»,

Правление Общества РЕШИЛО:

1. Утвердить Политику информационной безопасности АО «Казахстанский центр государственно-частного партнерства», согласно приложению, к настоящему решению.

2. Директору департамента административно-правового обеспечения Ысқақ Ә.Б., принять необходимые меры, вытекающие из настоящего решения.

3. Настоящее решение вступает в силу с момента его подписания.

Выписка верна

Секретарь Правления **Б. Булатова**

Приложение №1
к решению Правления
АО «Казахстанский центр
государственно-частного партнерства»
от «28» декабря 2021 года № 50

	Вышестоящий документ	Законы РК: «О национальной безопасности», «Об информатизации», «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности (постановление ПРК от 20.12.2016 г. №832)
	Владелец документа	АО «Казахстанский центр государственно-частного партнерства»
	Разработал	Департамент административно-правового обеспечения АО «Казахстанский центр государственно-частного партнерства»
	Утверждено	Решением Правления АО «Казахстанский центр государственно-частного партнерства» от «__»_____2021г.
	Дата вступления в силу	«____»_____2021 год
	Гриф ограничения	Для служебного пользования

Политика информационной безопасности акционерного общества «Казахстанский центр государственно-частного партнерств

г. Нур-Султан, 2021 год

СОДЕРЖАНИЕ:

Глава 1. Общие положения

1. Настоящая Политика информационной безопасности Акционерного общества «Казахстанский центр государственно-частного партнерства» (далее – Политика) предназначена для определения основных требований обеспечения информационной безопасности в деятельности АО «Казахстанский центр государственно-частного партнерства» (далее – Общество) и представляет собой систематизированное изложение целей и задач, основных руководящих принципов, организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

2. Приоритетными направлениями в процессе обеспечения информационной безопасности Общества являются:

1) выявление, предупреждение и пресечение утечки и утраты служебных сведений, в том числе составляющих государственные секреты и иную защищаемую законом тайну;

2) поддержание и развитие эффективной системы защиты информационных ресурсов, информационных систем и инфраструктуры связи, в которых циркулируют служебные сведения, в том числе составляющие государственную и иную защищаемую законом тайну.

3. Информационная безопасность в Обществе обеспечивается посредством реализации комплекса превентивных мер по защите служебной информации, в том числе ограниченного распространения. Должный уровень защиты достигается исключительным выполнением всех установленных требований, процедур, организации структуры и функций программного и аппаратного обеспечения, а также контроля их соблюдения со стороны всех участников информационных процессов.

4. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности.

5. Положения Политики распространяются на структурные подразделения Общества и на службу технической поддержки, в которых осуществляется автоматизированная обработка информации и использование средств вычислительной техники (далее – СВТ).

6. В настоящей Политике используется понятийный аппарат (термины, определения), соответствующий основным терминами и определениям, установленным в действующем законодательстве Республики Казахстан в сфере информационной безопасности.

7. При выдаче СВТ работникам Общества подразделение материального обеспечения, обеспечивает ознакомление работников Общества с настоящей Политикой.

Глава 2. Цели и задачи Политики

8. Целью настоящей Политики является определение общих требований к организации системы управления информационной безопасностью Общества посредством применения соответствующих методик и аппаратно-программных комплексов, реализации выработанных регламентов и процедур.

9. Функционально система управления информационной безопасностью призвана обеспечить и поддерживать:

1) конфиденциальность информации, хранящейся и обрабатываемой средствами вычислительной техники и передаваемой по каналам связи;

2) целостность и аутентичность информации, хранящейся и обрабатываемой в информационной системе Общества и передаваемой по каналам связи;

3) доступность хранящейся и обрабатываемой информации пользователям;

4) устойчивое функционирование информационно-коммуникационной инфраструктуры (далее – ИКИ) Общества.

Эффективность и надежность системы управления информационной безопасностью оценивается ее способностью предотвращения, исключения или минимизации ущерба от инцидентов информационной безопасности (процессы управления рисками).

10. Для достижения цели Политики необходимо решение следующих задач:

1) активное участие руководства Общества в управлении информационной безопасностью Общества;

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

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

4) формирование и проведение в Обществе единой политики в области обеспечения информационной безопасности;

5) обеспечение бесперебойной работы Общества и сведение к минимуму экономического, финансового, социального, институционального и экологического ущербов от реализации угроз информационной безопасности посредством их предотвращения и/или сведение последствий к минимуму;

6) определение процедур, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

7) определение требований к содержанию процедур по управлению информатизацией Общества с учетом необходимости решения задач обеспечения информационной безопасности;

8) координация деятельности Общества при проведении работ в ИКИ Общества с соблюдением требований стандартов обеспечения информационной безопасности;

9) повышение уровня защищенности ИКИ Общества;

10) разработка предложений по совершенствованию правового, методического, технического и организационного обеспечения информационной безопасности Общества.

Глава 3. Основные руководящие принципы обеспечения информационной безопасности

11. Основными принципами обеспечения информационной безопасности в Обществе являются:

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 информационных активов;

4) выявление причинно-следственных связей возникающих проблемных ситуаций и построение на этой основе точного прогноза их развития;

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. Защита обеспечивается физическими средствами, организационными, технологическими и правовыми мерами. При этом меры, принимаемые для обеспечения информационной безопасности, не усложняют достижение основных стратегических целей Общества, а также не повышают трудоемкость технологических процессов обработки информации;

6) эффективная реализация принятых защитных мер;

7) гибкость средств защиты для обеспечения варьирования уровнем защищенности в связи с возможными изменениями внешних условий и требований с течением времени;

8) совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования информационных систем с учетом изменений в методах и средствах перехвата информации и воздействия на их компоненты, нормативных требований по защите, достигнутого в этой области опыта других организаций, как отечественных, так и зарубежных;

9) необходимость и своевременность выявления, пресечения попыток нарушения установленных правил обеспечения информационной безопасности;

10) определение функциональных целей и целей информационной безопасности в документах во избежание неопределенности в организационной

структуре, ролей работников, утвержденных политик и невозможности оценки адекватности принятых защитных мер;

11) определение персональной ответственности за обеспечение безопасности информации и системы ее обработки для каждого работника в пределах его полномочий.

Глава 4. Организация обеспечения информационной безопасности

12. Синхронизация часов, всех соответствующих средств обработки информации внутри Общества определяется с помощью единого источника, заданного по точному времени города Нур-Султан (применяется как Универсальное скоординированное время – UTC). Единая интерпретация формата времени: час, минут, день, месяц, год.

13. К участникам подлежащих контролю и защите информационных процессов относятся:

1) пользователи – работники Общества, имеющие авторизованный доступ к электронным информационным ресурсам Общества, осуществляющие свою деятельность и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;

2) служба технической поддержки – обслуживающий и технический персонал;

14. Защите подлежат информационные ресурсы, циркулирующие в ИКИ Общества.

Глава 5. Меры по реализации Политики

15. Пользователи, работающие в ИКИ Общества, обеспечивают соблюдение установленных требований настоящей Политики.

16. Лицо, ответственное за обеспечение ИБ, осуществляет:

1) разработку нормативно-технической документации в области информационной безопасности и дальнейший контроль исполнения требований по информационной безопасности;

2) контроль за документальным оформлением;

3) контроль за управлением активами в части обеспечения информационной безопасности;

4) контроль законности использования программного обеспечения;

5) контроль за управлением рисками (оценка рисков);

6) координацию и контроль за регистрацией событий информационной безопасности;

7) проведение планового и внепланового аудита информационной безопасности;

8) организацию и контроль за проведением внешнего аудита информационной безопасности;

9) контроль за обеспечением непрерывности бизнес-процессов и его осуществлением;

10) контроль за соблюдением требований информационной безопасности при управлении персоналом;

11) контроль за состоянием информационной безопасности информационных систем на всех этапах жизненного цикла;

12) участие в мероприятиях по анализу использования информационно - коммуникационных технологий (далее – ИКТ) - активов;

13) участие при внедрении аппаратных и программных средств обеспечения информационной безопасности;

14) согласование требований к информационной безопасности в процессе создания, развития и применения информационных систем;

15) участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию.

17. Реализацию задач в сфере информатизации в Обществе обеспечивает лицо ответственное за обеспечение ИБ, осуществляющее:

1) мониторинг и анализ применения ИКТ;

2) разработку технической документации по информационной безопасности по согласованию с лицом, ответственным за обеспечение ИБ.

3) участие в мероприятиях по учету и анализу использования ИКТ - активов;

4) выработку предложений по вопросам информатизации;

5) координацию работ по созданию, сопровождению и развитию объектов информатизации;

6) реализацию требований по информационной безопасности;

7) обеспечение надежности функционирования системы защиты;

8) участие при внедрении аппаратных и программных средств обеспечения информационной безопасности;

9) участие в формировании требований к информационной безопасности в процессе создания, развития и применения информационной системы;

10) участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;

11) обеспечение функционирования (непрерывной работы) активов, связанных со средствами обработки информации;

18. Распределение прав и обязанностей работников выстраивается таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

19. Контроль деятельности пользователей, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает как несанкционированные, так и санкционированные действия пользователей.

20. Предоставление доступа к информационным системам пользователю допускается только после ознакомления с действующими требованиями

информационной безопасности.

Глава 6. Оценка рисков информационной безопасности

21. С целью управления рисками в сфере применения ИКТ Общества осуществляется оценка рисков в соответствии со стандартом Республики Казахстан СТ РК 31010-2010 «Менеджмент риска. Методы оценки риска».

22. Целью оценки рисков информационной безопасности является получение объективной информации о возможных нарушениях бизнес-процессов и их последствиях или иного ущерба по причине нарушения требований информационной безопасности.

23. Оценка рисков информационной безопасности, с точки зрения управления рисками, определяется как анализ систематически подвергающихся угрозам и существующим уязвимостям информационных ресурсов и систем с применением существующих научных методов и средств.

24. Оценка рисков основывается на определении величины рисков и процессе сравнения оцененных рисков с критериями рисков с целью установления их значимости (оценка степени рисков). Оценка рисков проводится по мере необходимости для реагирования на изменения в требованиях информационной безопасности и в ситуации рисков.

Глава 7. Идентификация, классификация и маркировка активов

25. Основные информационные активы Общества учитываются и закрепляются за ответственными лицами (пользователями согласно паспортным данным актива и обслуживающим подразделением).

26. Для всех категорий пользователей активов определяется их ответственность за поддержание соответствующих мероприятий по управлению информационной безопасностью.

27. Каждый актив подлежит четкой идентификации и классификации с точки зрения безопасности, его пользователи проходят процедуру авторизации, а данные о них документируются с указанием фактического местоположения актива (в соответствии с паспортными данными актива).

28. Перечень (реестр) оборудования и программного обеспечения составляется и поддерживается в актуальном состоянии для всех активов, связанных с используемыми в Обществе информационными ресурсами и системами.

Глава 8. Обеспечение непрерывной работы активов

29. С целью минимизации до приемлемого уровня отрицательных последствий, вызванных нарушениями информационной безопасности, подразделением информационных технологий обеспечивается непрерывность

функционирования информационных процессов, действующих в Обществе, посредством применения комплекса организационных и технических мероприятий по управлению информационной безопасностью.

30. Для обеспечения непрерывной работоспособности активов проводится определение критических активов и соответствующих требований к непрерывности их работы, включающие в себя:

1) основные меры, методы и средства сохранения (поддержания) работоспособности ИКИ Общества,

2) способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности информационных активов и их основных компонентов

3) разработку плана мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации, реализация которого нацелена на своевременное обнаружение и локализацию в течение требуемого времени причин возникновения нештатных ситуаций.

31. Поддержка целостности, доступности информации и средств ее обработки предусматривает проведение регулярных процедур резервирования, формирования копий данных и тестирования, их своевременного восстановления.

Глава 9. Инвентаризация и паспортизация активов

32. Инвентаризация и паспортизация активов осуществляется в целях создания единой информационной базы средств вычислительной технике, телекоммуникационного оборудования и программного обеспечения, эксплуатируемых в Обществе, в том числе используемых работниками Общества.

33. Инвентаризация, паспортизация и порядок использования активов, закрепление активов за конкретными должностными лицами и определение меры их ответственности в соответствии с законодательством Республики Казахстан за соблюдение требований информационной безопасности в совокупности составляют основу обеспечения защиты этих активов.

Глава 10. Внутренняя проверка информационной безопасности

34. Под проверкой информационной безопасности понимается процесс получения объективной оценки текущего состояния информационной безопасности в соответствии с определенными критериями и показателями. Правильное представление о текущем уровне защищенности является основой для построения эффективной системы управления информационной безопасностью.

35. Проверка необходима для обеспечения постоянной пригодности и эффективности применяемых подходов в процессах управления информационной безопасностью. Проверка включает оценку возможностей для улучшения и необходимости изменений в методах обеспечения безопасности, включая политику, цели и меры управления.

36. Проверка проводится ответственным лицом за информационную безопасность и соблюдения требований информационной безопасности.

37. Проверка проводится согласно потребностям и в случае возникновения инцидентов нарушения информационной безопасности, существенного повышения вероятности осуществления рисковых событий.

Глава 11. Права доступа к электронным информационным ресурсам

38. Разграничение прав доступа является одной из основных мер по обеспечению защиты электронных информационных ресурсов Общества.

39. Для контроля, за предоставлением права доступа к информационным системам и сервисам предусматривается ряд формализованных процедур, охватывающих стадии цикла пользовательского доступа от начальной регистрации новых пользователей, до конечного снятия с регистрации пользователей, которым больше не требуется доступ к информационным системам, сервисам и СВТ.

Подразделением информационной безопасности осуществляется контроль за исполнением мероприятий в отношении предоставления прав привилегированного доступа, с помощью которых пользователи могут обходить системные средства контроля.

40. В многопользовательских системах (операционная система, система управления базой данных, информационные системы) обеспечивается контроль использования привилегированных прав доступа. Привилегии ограничены и идентифицированы в отношении каждого системного продукта, программного обеспечения и каждой категории работников, которым эти привилегии предоставляются.

41. Доступ к ресурсам предоставляется только для выполнения административных обязанностей.

42. Для соблюдения принципа персональной ответственности каждому пользователю, допущенному к работе с электронным информационным ресурсом Общества, присваивается персональное уникальное имя (учетная запись пользователя) с паролем в соответствии с единым форматом присвоения имен учетным записям.

43. При изменении должности или функциональных обязанностей работника удаляются имеющиеся права доступа и присваиваются новые, в соответствии с необходимым функционалом. При увольнении работника удаляются его права доступа в информационные системы и СВТ, не позднее дня увольнения, а также устанавливается порядок временной приостановки прав

доступа в информационные системы, при длительном отсутствии работника.

44. При предоставлении доступа к информационной системе Общества сторонним организациям, а также при интеграции с информационной системой Общества с информационной системой государственных органов Республики Казахстан учитываются обязательные условия соблюдения конфиденциальности данных требований ИБ.

45. Права доступа пользователей подлежат регулярному пересмотру. Причиной внепланового пересмотра прав доступа служит изменение штатной расстановки, изменение перечня сервисов сети и электронных информационных ресурсов, изменение политики информационной безопасности, выявленные факты нарушений или не эффективное использование соответствующих прав доступа.

Глава 12. Интернет и электронная почта

46. Под безопасностью работы с интернетом и электронной почтой понимается защищенность электронной информации, передаваемой по электронной почте и каналам сети интернет, от случайных или преднамеренных воздействий естественного или искусственного характера, утечки, хищения, утраты, уничтожения, искажения, копирования, подделки, блокирования информации и других угроз, возникающих в результате несанкционированного доступа, а также некорректного использования или не соблюдения необходимых требований.

Глава 13. Организация процедуры аутентификации

47. Надежная аутентификация является одним из ключевых факторов, гарантирующих, что только авторизованные пользователи получают доступ к контролируемой информации.

48. За каждым СВТ закрепляется работник Общества. На СВТ используется система аутентификации и идентификации работника, работающего на нем.

49. В целях идентификации, аутентификации и соблюдения принципа персональной ответственности, в Обществе пользователям присваиваются персональные уникальные имена с паролями (идентификатор, учетная запись).

Уникальный идентификатор пользователя позволяет обеспечить его единоличное использование, отслеживать и анализировать действия пользователя на предмет соблюдения требований технической документаций по информационной безопасности.

50. Контроль действий применяется для всех категорий пользователей (включая персонал службы технической поддержки).

51. Пароли являются наиболее распространенными средствами подтверждения идентификатора пользователя при доступе к информационной

системе или сервису.

При необходимости рассматривается возможность использования других технологий для идентификации и аутентификации пользователя, таких как биометрия (проверка отпечатков пальцев, радужной оболочки глаз, фотоизображение лица и так далее), электронная цифровая подпись, аппаратные средства идентификации (чип-кары, микросхемы).

52. При формировании паролей учитываются требования, описанные в Порядке организации процедуры аутентификации.

53. Пользователь не разглашает и не передает полученные идентификаторы. Пользователь дает письменное подтверждение об ознакомлении с правами доступа, ответственности по неразглашению информации, понимании условий и требований предоставления прав доступа.

Глава 14. Антивирусная защита

54. Антивирусная защита информации осуществляется посредством применения организационных мероприятий, административных мер и программных антивирусных средств, для предотвращения заражения вредоносными программами (вирусами) объектов информатизации.

55. В Обществе защита от вредоносного программного обеспечения, основанная на применении антивирусных средств, направлена на предотвращение уничтожения, модификации, хищения и несанкционированного использования важной служебной информации. К использованию допускаются только лицензионные антивирусные средства.

56. Антивирусные средства обнаружения вирусов применяются для проверки серверов, рабочих станций, носителей информации и иных активов на наличие вирусов.

57. Мониторинг работоспособности антивирусных средств, вирусной активности, а также обновление антивирусных баз службой поддержки проводятся ежедневно.

58. Процесс выбора антивирусного программного обеспечения проводится с обязательным участием подразделения информационных технологий и подразделения информационной безопасности.

Глава 15. Использование мобильных устройств и носителей информации

59. Мобильные устройства являются важной частью ИКИ Общества, одновременно выступая источником уникальных угроз и рисков в силу их использования за пределами корпоративной системы защиты (вне локальной вычислительной сети), что повышает риски информационной безопасности. При этом возникает необходимость соизмерять требуемую защиту со специфичными рисками работы.

60. При использовании мобильных устройств и носителей информации в

Обществе учитываются риски, связанные с работой в незащищенной среде, и применяются соответствующие меры защиты. Дистанционный режим безопасной работы обеспечивается реализацией комплекса мероприятий организационного и технологического характера, предусматривает применение программно-аппаратных средств защиты и обеспечения информационной безопасности.

61. Работниками Общества не допускается фото и видеосъемка проектов документов, а также самих документов Общества, используемых в работе.

62. Мобильные устройства и носители информации Общества учитываются и персонально закрепляются за ответственными лицами (пользователями).

63. Информация об использовании работниками Общества мобильных устройств и носителей информации протоколируется путем периодических проверок.

Глава 16. Организация физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов

64. Зону информационной безопасности необходимо защищать с помощью соответствующих мер контроля входа для обеспечения доступа только авторизованному персоналу.

65. Способы размещения и защиты средств обработки информации предусматривают минимизацию рисков от воздействий окружающей среды и возможности неавторизованного доступа. На регулярной основе проводится актуализация учетных данных всех средств вычислительной техники (реестр оборудования) с проверкой соответствия конфигураций с паспортными сведениями.

66. В целях обеспечения должного уровня безопасности и непрерывности бизнес-процессов в Обществе предусмотрены меры на следующих направлениях:

1) защита сетей телекоммуникации от перехвата или повреждения передаваемой информации, постоянный мониторинг за возможными изменениями в их топологии и структуре;

2) непрерывный контроль работы программно-аппаратных средств обеспечения сетевой безопасности (межсетевых экранов, отдельных шлюзов доступа, оборудования сегментации сетей, демилитаризации зон и так далее);

3) мониторинг режимов функционирования систем жизнеобеспечения (электропитание, кондиционирование, пожаротушение, видеонаблюдение и тому подобное), их надлежащего технического обслуживания для обеспечения непрерывной работоспособности и целостности;

4) обеспечение гарантированного уничтожения информации с носителей информации при выводе оборудования из эксплуатации;

5) контроль строгого соблюдения необходимых требований при осуществлении процессов вноса/выноса оборудования в/из административного здания.

67. На узлах информационной инфраструктуры необходимо контролировать целостность настроек безопасности, важных системных и конфигурационных файлов.

68. Необходимо проводить организационные мероприятия и, при необходимости, устанавливать программно-технические средства, снижающие риск доступа к информационной инфраструктуре неавторизованных конечных устройств, либо устройств, настройки которых противоречат установленным организацией правилам обеспечения информационной безопасности.

69. Необходимо использовать групповые политики безопасности, позволяющие автоматически устанавливать на всех конечных устройствах и узлах информационной инфраструктуры необходимые настройки безопасности.

70. Перед вводом программного обеспечения в эксплуатацию необходимо провести следующую экспертизу:

1) в службе информационных технологий на предмет совместимости с остальным программным обеспечением, используемым организацией;

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

71. Подразделения информационной безопасности и информационных технологий отслеживают выход обновлений информационных систем, публикации о выявленных уязвимостях в используемых Обществом информационных системах и определяют политику управления обновлениями.

72. Защита СВТ пользователей от несанкционированного доступа в Обществе строится по нескольким направлениям:

1) создание автоматизированных средств регистрации пользователей;

2) система блокирования учетных записей;

3) оповещение работников об угрозе или проникновении в СВТ.

73. Определяется организационные меры по предотвращению несанкционированного доступа (далее – НСД), в том числе в случае утраты/компрометации паролей и выхода из строя СВТ.

74. Защита информации от утечки по каналам их передачи в Обществе достигается путем применения комплексных программных, технических средств защиты и организационных мер.

75. Для защиты средств обработки информации и безопасной среды функционирования информационных ресурсов в Обществе кроме мероприятий, включающих физическую защиту, проведение аудита обращения к СВТ и мониторинг системных журналов, устанавливается базовый комплекс программного обеспечения.

Базовый комплекс устанавливается на рабочие места пользователей и включает в себя лицензионное программное обеспечение (далее – ПО),

необходимое для обеспечения работоспособности СВТ.

76. Использование для производственных целей прикладного ПО, не входящего в состав базового комплекса производится по согласованию с подразделением информационной безопасности.

77. Защита коммуникаций от незаконного подключения, кроме средств санкционированного электронного и физического доступа, осуществляется программными, техническими средствами и организационными мерами. Проводятся мероприятия для своевременного выявления, предупреждения и пресечения неправомерных действий лиц по получению доступу к коммуникациям.

78. Обществом определяется порядок резервного копирования, хранения и восстановление программных продуктов и информационных систем.

79. При передаче СВТ на ремонт и сторонние организации следует принять исчерпывающие меры защиты информации на устройствах долговременной памяти.

80. Подготовка по улучшению осведомлённости имеет целью дать возможность отдельным лицам распознавать проблемы информационной безопасности и инциденты её нарушения и реагировать соответственно своим рабочим обязанностям.

Глава 17. Пересмотр Политики

81. Политика пересматривается с целью анализа и актуализации изложенной в ней информации не реже одного раза в два года.

82. Пересмотр Политики производится в целях:

1) совершенствования форм и методов контроля информационной безопасности;

2) совершенствования подходов к управлению информационной безопасностью и бизнес-процессами Общества;

3) улучшения распределения ресурсов и/или обязанностей.

83. Политика пересматривается в соответствии с изменениями, влияющими на основу предыдущей оценки риска, с учетом выявленных существенных инцидентов нарушения информационной безопасности, появления новых уязвимостей или изменения организационной/технологической инфраструктуры, изменения основных характеристик бизнес-процессов Общества, а также существенных изменений в технологиях, обеспечивающих информационную безопасность.

84. Замечания и предложения со стороны пользователей к изменениям норм Политики анализируются подразделением информационной безопасности и при необходимости учитываются в пересматриваемой Политике.

85. Политика пересматривается в случае изменения общих политик безопасности информации, пересмотра ее ценности.

Глава 18. Меры по недопущению предоставления удаленного доступа к информационным ресурсам Общества

86. В Обществе не допускается использование программных средств организации удаленного доступа из сети интернет в информационно-коммуникационной среде Общества.