НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«ЗАПАДНО-КАЗАХСТАНСКИЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ
ИМЕНИ МАРАТА ОСПАНОВА»

УТВЕРЖДЕНО
Решением Правления
НАО «Западно-Казахстанский медицинский
университет имени Марата Оспанова»
протокол № 10
от 21.11 **2022 год**

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАО «ЗАПАДНО-КАЗАХСТАНСКИЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ ИМЕНИ МАРАТА ОСПАНОВА»

Код	Издание	Разработал(а)	Согласовано	Подпись	Дата
П ЗКМУ 63-15	Первое	Мусина М.А. 18 11 2022 г.	Урумбаева А.Н.		21.11.2022

Актобе, 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ И ОСНОВНЫЕ ПОНЯТИЯ

1.1. В настоящей политике информационной безопасности (далее - Политика) определен комплекс мер по предотвращению, обнаружению и решению проблем с целью защиты целостности, конфиденциальности и доступности обрабатываемых данных на объектах информатизации НАО «Западно-Казахстанский медицинский университет им.М.Оспанова» (далее – Университет).

1.2. Политика является документом первого уровня технической документации по информационной безопасности и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения информационной безопасности.

1.3. Политика разработана в соответствии с требованиями Закона Республики Казахстан от 24 ноября 2015 года «Об информатизации», Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утверждёнными Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 и другими нормативными правовыми и техническими актами в части обеспечения информационной безопасности.

1.4. В случае привлечения сторонних организаций к обеспечению информационной безопасности электронных информационных ресурсов, информационных систем, информационно-коммуникационных инфраструктур, их собственник или владелец заключает соглашения, в которых устанавливаются условия работы, доступа или использования данных объектов, а также ответственность за их нарушение.

2. ЦЕЛЬ ПОЛИТИКИ

2.1. Целью Политики является:

1) определение технических и процедурных мер для обеспечения исполнения законодательства и нормативно-технической документации в области информационной безопасности;

2) определение средств, позволяющих обеспечить безопасность, а также предотвратить несанкционированный доступ, изменение, публикацию, удаление и повреждение обрабатываемых данных;

3) обеспечение непрерывности основных процессов Университета для сохранения стабильности функционирования объектов информатизации;

4) минимизация возможных потерь и ущерба от нарушений в области информационной безопасности.

2.2. Основными направлениями обеспечения информационной безопасности являются:

- принятие мер по защите конфиденциальности, целостности и доступности всех значимых для Университета активов объектов информатизации;
- управление рисками информационной безопасности и их поддержание в пределах утвержденного руководством Университета уровня приемлемости на основе системы оценки рисков;
- поддержание необходимого уровня знаний, навыков и участия всех сотрудников Университета в области обеспечения информационной безопасности.

3. ПЕРЕСМОТР ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Политика и техническая документация по информационной безопасности пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в три года, а также по инициативе руководства Университета, с целью обеспечить ее соответствие изменениям в законодательстве. В случае пересмотра Политики в документы, которые ссылаются на данную Политику, также подлежат пересмотру.

3.2. Главными инструментами обеспечения соответствия является периодический пересмотр внутренних норм и индивидуальная корректировка внутренних норм и правил в случае внесения значительных изменений во внешнюю нормативно-правовую базу.

3.3. Корректировка внутренних норм и правил в результате изменения внешней нормативно-правовой базы должна проводиться в срок до 3 месяцев с момента такого изменения.

4. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

4.1. Система управления информационной безопасностью остается действенной и эффективной в долгосрочном периоде в процессе внутренних и внешних изменений. Внешние изменения связаны с законодательством и изменениями в условиях среды, внутренние изменения вносятся с учетом анализа информационной безопасности. Процесс реализуется с учетом цикличного пересмотра нормативов информационной безопасности. Данный цикл имеет следующие этапы:

1) планирование - определение целей информационной безопасности, проектирование процессов, оценка рисков информационной безопасности, выбор соответствующих средств контроля и их детализация;

2) действие - реализация средств контроля и внедрение процессов информационной безопасности в действие;

3) проверка - пересмотр и оценка эффективности процессов и средств контроля;

4) корректировка - внесение поправок и изменений там, где это необходимо, для приведения средств контроля информационной безопасности в соответствие установленным целям безопасности.

4.2. В реализации системы управления информационной безопасностью используется подход на основе управления рисками в целях наиболее эффективного использования ресурсов для достижения максимального результата.

5. ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Университет:

- определяет общую формулировку целей и требований к информационной безопасности, отраслевую политику и нормативные требования;
- организует проверку эффективности систем информационной безопасности;
- утверждает планы по усовершенствованию и функционированию систем информационной безопасности;
- проводит проверку соблюдения требований информационной безопасности в структурных подразделениях;
- в пределах компетенций принимает решение по вопросам наложения дисциплинарного взыскания на сотрудников и работников учреждений и организаций в случае нарушения требований информационной безопасности.

5.2. Структурные подразделения, занимающиеся вопросами создания, сопровождения и развития объектов информатизации, осуществляют:

1) мониторинг и анализ применения объектов информатизации;

2) участие в мероприятиях по учету и анализу использования объектов информатизации;

3) выработку предложений в стратегический план Университета по вопросам информатизации;

4) координацию работ по созданию, сопровождению и развитию информационных систем Университета;

5) контроль за обеспечением поставщиками предусмотренного договорами уровня качества оказываемых услуг в сфере информатизации;

6) взаимодействие с сервисным интегратором, оператором, государственными и местными исполнительными органами, организациями в части реализации проектов в сфере информатизации при создании архитектуры и реализации сервисной модели информатизации;

7) реализацию требований по информационной безопасности.

Департамент цифровизации и автоматизации процессов детализирует технические и прочие средства контроля в целях обеспечения соответствия требованиям к информационной безопасности.

5.3. Отдел информационной безопасности и должностные лица, ответственные за обеспечение информационной безопасности, осуществляют:

1) контроль исполнения требований технической документации по информационной безопасности;

2) контроль за документальным оформлением по информационной безопасности;

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

4) контроль правомерности использования программного обеспечения;

5) контроль за управлением рисками в сфере информационно-коммуникационные технологии;

6) контроль за регистрацией событий информационной безопасности;

7) проведение внутреннего аудита информационной безопасности;

8) контроль за организацией внешнего аудита информационной безопасности;

9) контроль за обеспечением непрерывности бизнес-процессов, использующих информационно-коммуникационные технологии;

10) контроль соблюдения требований информационной безопасности при управлении персоналом;

11) контроль за состоянием информационной безопасности информационных систем.

12) Разрабатываются внутренние нормы информационной безопасности в соответствии с нормативными требованиями действующего законодательства, определяются меры ответственности сотрудников и работников в случае нарушения требований информационной безопасности.

6. МОНИТОРИНГ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Для наблюдения за информационными системами Университета с целью выявления угроз и инцидентов информационной безопасности, а также принятия мер по их устранению и предупреждению необходимо вести мониторинг обеспечения информационной безопасности.

6.2. Мониторинг обеспечения информационной безопасности (далее – МОИБ) осуществляется в соответствии с нормами законодательства Республики Казахстан и Правилами проведения мониторинга обеспечения информационной безопасности объектов информатизации и критически важных объектов информационно-коммуникационной инфраструктуры, утвержденных университетом.

6.3. Необходимо вести журналирование событий информационной безопасности с определением ответственных должностных лиц.

Элементы журнала информационных систем передаются в соответствующие структурные подразделения для сохранения и резервного копирования.

6.4. Архивирование журнала производится ежегодно.

6.5. В случае выявления нарушения системы безопасности, которое может повлечь потерю данных или факт раскрытия информации, следует информировать отдел информационной безопасности.

6.6. При управлении журналами устанавливаются следующие нарушения системы безопасности:

1) некорректная работа системы (возможно в результате внешней атаки);

2) некорректная работа оборудования (возможно вызывающая перебои в работе приложений);

3) некорректная работа компонента программного обеспечения, которая может стать причиной; некорректной передачи данных или перебоев в работе приложений;

4) несанкционированный доступ к функциям или данным;

5) недостаточная передача данных.

6.7. Любой доступ к конфигурации журналов в приложениях и оборудования инфраструктуры, или в хранилище журналов расценивается как инцидент в системе безопасности и подлежит расследованию отделом информационной безопасности для недопущения несанкционированного изменения процесса регистрации.

7. ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИДЕНТИФИКАЦИЯ, КЛАССИФИКАЦИЯ И МАРКИРОВКА АКТИВОВ

7.1. Все активы, связанные со средствами обработки данных Университета, закрепляются за определенными ответственными должностными лицами.

7.2. Активы делятся на следующие категории:

1) информационные активы (базы данных, нормативные документы, справочная информация, организационная информация, кадровая информация, данные о контрактах и так далее);

2) физические активы (технические средства обработки информации, программное обеспечение, съемные носители, вспомогательное оборудование, оборудование системы безопасности, здания, персонал).

7.3. Инвентаризация активов включает их основные технические параметры. Активы классифицируются по степени ценности и конфиденциальности информации, которую они хранят или обрабатывают.

7.4. Детальная формулировка требований содержится в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации.

8. УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

8.1. Для обеспечения информационной безопасности проводится регулярная оценка, анализ и управление рисками информационной безопасности.

8.2. Результаты процесса управления рисками информационной безопасности являются основой для выработки средств контроля информационной безопасности и Плана непрерывности бизнес-процессов.

8.3. Управление рисками информационной безопасности способствует повышению уровня защиты конфиденциальности, целостности и доступности информации. Управление рисками информационной безопасности осуществляется в соответствии с принятой методологией, с проведением обязательных процессов и использованием общих шаблонов;

8.4. Оценка и анализ рисков информационной безопасности проводится совместно структурными подразделениями по информационным технологиям и информационной безопасности. По результатам оценки и анализа рисков осуществляется планирование средств контроля с указанием уровней риска, которые необходимо достичь.

8.5. По результатам оценки и анализа рисков осуществляется планирование средств контроля с указанием уровней риска, которые необходимо достичь. Затраты на внедрение новых и совершенствование имеющихся средств контроля не должны превышать размер потенциального ущерба, вызванного соответствующими угрозами. Необходимо оценивать воздействие внедренных средств контроля на уровень риска (остаточный риск).

8.6. Детальная формулировка требований содержится в Методике оценки рисков информационной безопасности.

9. НЕПРЕРЫВНАЯ ДЕЯТЕЛЬНОСТЬ

9.1. Средства контроля информационной безопасностью обеспечивают необходимый уровень доступности к объектам информатизации Университета.

9.2. С целью определения способов продолжения оказания ограниченного объема услуг и восстановления первоначальных операционных условий разрабатываются и постоянно

обновляются планы действий в непредвиденных ситуациях, при временной остановке функционирования систем.

9.3. Принципы обеспечения непрерывной деятельности:

1) соответствие принимаемых мер ожиданиям структурным подразделениям Университета на основании совместного анализа последствий для деятельности;

2) обеспечение избытка технической среды и закупаемых услуг третьих сторон, если заявленные ожидания со стороны бизнеса невозможно удовлетворить иным образом;

3) обеспечение приемлемого операционного уровня процедур непрерывности бизнес-процессов (даже в случаях приостановления функционирования объектов информатизации Университета).

4) разработка отделом информационной безопасности совместно с департаментом цифровизации и автоматизации процессов процедур после аварийного восстановления поврежденных технических компонентов объектов информатизации Университета;

5) хранение в течение трех лет документов по возникшим чрезвычайным ситуациям и принятым мерам по их ликвидации.

9.4. Детально требования определены в Правилах по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

10. ИНВЕНТАРИЗАЦИЯ И ПАСПОРТИЗАЦИЯ ОБОРУДОВАНИЯ

10.1. В соответствии с требованиями Закона Республики Казахстан «Об информатизации» от 24 ноября 2015 года и Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832.

10.2. Собственник, владелец ведет и ежегодно обновляет инвентарные ведомости для данного оборудования.

10.3. Принципы инвентаризации и паспортизации оборудования:

1) соответствие инвентарной ведомости реестру активов;

2) соответствие инвентарной ведомости данным финансового учета;

3) учет в процессе инвентаризации изменений жизненного цикла оборудования и информационных систем.

10.4. Детальная формулировка требований определена в Правилах инвентаризации и паспортизации вычислительной техники, телекоммуникационного оборудования и программного обеспечения.

11. ВНУТРЕННИЙ АУДИТ

11.1. В целях контроля Университет самостоятельно осуществляет внутренний аудит по информационной безопасности.

Порядок проведения внутреннего аудита (контроля) определяется Законом Республики Казахстан «Об административных процедурах» с учетом требований Правил проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 февраля 2018 года № 33/НҚ, Критериев оценки степени риска и проверочных листов в сфере информатизации в части обеспечения информационной безопасности, утвержденных совместным приказом заместителя Премьер-Министра Республики Казахстан - Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года № 12.

11.2. Функционирование информационных систем Университета подлежит внутреннему аудиту с точки зрения информационной безопасности для проверки соблюдения требований Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утверждённых постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

11.3. Принципы внутреннего аудита:

1) соответствие системы управления информационной безопасности рекомендациям стандартов СТ РК ISO/IEC 27001-2015 и СТ РК ISO/IEC 27002-2015;

2) непрерывность процесса аудита в соответствии с годовым планом;

3) обоснованность годового плана аудита результатами оценки информационных рисков;

4) объективность контрольно-аудиторского процесса;

5) обеспечение аудитора правом запроса необходимой документации и информации, связанной с проверяемой областью деятельности;

6) предоставление аудиторского заключения по результатам аудита руководству Университета;

7) контроль отделом информационной безопасности исполнения рекомендаций аудиторов и предоставление отчета о степени исполнения руководству Университета.

11.4. Детальная формулировка требований содержится в Правилах проведения внутреннего аудита информационной безопасности.

12. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА УПРАВЛЕНИЯ

12.1. В случаях, когда это оправдано характером определенного информационного актива, хранение и передача информации их защита осуществляется с использованием криптографических средств управления.

12.2. Криптографические средства управления включают шифрование информации с целью сохранения конфиденциальности и (или) использование цифровой подписи с целью обеспечения целостности информации.

12.3. Принципы криптографического управления:

1) обеспечение защиты конфиденциальности и целостности информации от применяемых методов взлома и обоснованно ожидаемых попыток их нарушения при применении криптографических средств управления;

2) применение к хранящимся и передаваемым данным криптографических средств управления;

3) применение криптографических средств управления к криптографическим ключам, съемным носителям и журналам безопасности информационных систем;

4) применение процедуры управления криптографическими ключами на протяжении их полного жизненного цикла;

5) оценка эффективности применения криптографических средств управления осуществляется не менее одного раза в год и проводится усиление средств управления при наличии технических возможностей.

12.4. Детальная формулировка требований содержится в Правилах использования средств криптографической защиты информации.

13. КОНТРОЛЬ ДОСТУПА

13.1. Контроль доступа осуществляется посредством процедур и технических средств предоставления доступа к объектам информатизации Университета, физическим лицам и компонентам информационных технологий.

13.2. Средства контроля физического доступа к данным компонентам описаны в разделе «Физические средства защиты».

13.3. Принципы контроля доступа:

1) реализация механизма контроля доступа в отношении каждого информационного и физического актива, кроме отнесенных к категории «открытые»;

2) рассмотрение каждого запроса в систему контроля доступа отдельно и утверждение в установленном порядке;

3) обоснованность контроля доступа на идентификации и авторизации по имени пользователя и паролю;

4) обязательность сохранять персоналом конфиденциальность учетных данных в системе контроля доступа;

5) необходимость внедрения процедуры разблокировки заблокированных учетных записей;

6) наличие двухэтапной авторизации в случае некоторых категорий конфиденциальных активов;

7) обеспечение доступа к информационным активам только для выполнения пользователем своих должностных обязанностей;

8) аннулирование права доступа к информации и средствам обработки информации, включающие физический и логический доступ, идентификаторы доступа, подписки, документацию, которая идентифицирует его как действующего служащего или работника организации, после прекращения его трудового договора или изменяются при внесении изменений в условия трудового договора;

9) ежегодный пересмотр прав доступа пользователей с целью выявления нарушений;

10) оценка попытки обойти средства контроля доступа как инцидента в системе безопасности с последующим расследованием;

11) обеспечение соблюдения требовании, установленных законодательством Республики Казахстан, при обработке и хранении служебной информация ограниченного распространения и государственных секретов;

12) контроль за особыми системными привилегиями.

13.4. Детальная формулировка требований содержится в Правилах разграничения прав доступа к электронным информационным ресурсам.

14. ДОСТУП К СЕТИ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТЕ

14.1. Рабочие станции, установленные в помещениях, подключаются к сети Интернет через единый шлюз доступа к Интернету и центральный межсетевой экран (файервол). Исключение допускается при использовании для коммуникации открытой мобильной сети.

14.2. Не допускается использование сети Интернет и электронной почты в личных целях (личной переписки, регистрации с целью получения услуг, подписки на личные рассылки и осуществления личных покупок, отправления и получения изображений, видео и презентаций в каких-либо целях, кроме служебных), кроме случаев угрозы жизни человека.

14.3. Фильтр спама устанавливается на Интернет-шлюзе с целью недопущения получения пользователями нежелательных электронных писем.

14.4. Передавать служебную информацию ограниченного распространения по техническим каналам открытых видов связи (телефонная, факсимильная связь общего пользования, радиосвязь, спутниковая и сотовая (подвижная (мобильная) связь, сеть Интернет) не допускается.

14.5. Служащим и работникам Университета для осуществления оперативного информационного обмена (служебной переписки) в электронной форме при исполнении ими служебных обязанностей допускается использовать только корпоративную:

- электронную почту;
- систему электронного документооборота «Documentolog»;
- модуль объявления в информационной системе «Платонус».

Корпоративная электронная почта Университета размещается в доменной зоне zkmu.kz.

14.6. Детальная формулировка требований содержится в Правилах использования Интернет и электронной почты.

15. ПРОЦЕДУРА АУТЕНТИФИКАЦИИ

15.1. Пользователь, получающий доступ к рабочим станциям и информационным системам Университета надлежащим образом идентифицируется и аутентифицируется.

При доступе к объектам информатизации первого и второго классов в соответствии с классификатором необходимо применять многофакторную аутентификацию, в том числе с использованием электронной цифровой подписи.

Электронный документ, удостоверенный посредством электронной цифровой подписи лица, имеющего полномочия на его подписание, равнозначен подписанному документу на бумажном носителе.

15.2. Целью аутентификации является установление личности с помощью фрагмента данных. В данном процессе могут использоваться три типа данных:

1) что-то известное (например, пароль);

2) что-то имеющееся (например, токен);

3) какая-то биологическая характеристика (например, отпечаток пальца).

15.3. Принципы аутентификации:

1) соответствие метода аутентификации для получения доступа к ресурсам степени конфиденциальности данного информационного ресурса. В случае доступа к особо конфиденциальной информации используются дополнительные средства аутентификации – карточка-ключ, токен или биометрические данные;

2) авторизация осуществляется с использованием уникального идентификатора пользователя и пароля;

3) использование общего идентификатора пользователей допускается только в исключительных случаях по согласованию с подразделениями информационной безопасности;

4) запрещено использовать групповые идентификаторы (например, гость) для получения доступа к информационным системам Университета. Допускается использовать для получения доступа к общим ресурсам (например, доступ к беспроводной сети Интернет для посетителей), если такой доступ согласован отделом информационной безопасности;

5) вновь выданные пароли используются временно и подлежат изменению при первом доступе к выбранному ресурсу, при этом данное изменение подлежит гарантированию техническими средствами;

6) сохранение конфиденциальности учетных данных для аутентификации является обязанностью пользователя;

7) обеспечение надежности используемых паролей с учетом сложности количества и набора символов;

8) недопустимость повторного использования паролей (подлежат регулярной смене, запрещено вновь использовать предыдущие 5 паролей);

9) не допускается отображать пароли пользователей на электронном или бумажном носителе, хранение и передача паролей осуществляется в зашифрованном виде;

10) после 5 неудачных попыток аутентификации учетная запись пользователя блокируется;

11) необходимо сообщать в подразделение информационной безопасности о фактах утери или взлома пароля, данные пароли подлежат смене в установленном порядке;

12) Детальная формулировка требований содержится в Правилах организации процедуры аутентификации.

16. АНТИВИРУСНЫЙ КОНТРОЛЬ

16.1. При организации доступа к Интернету из локальных сетей внешнего контура в обязательном порядке обеспечивается наличие антивирусных средств, обновлений операционных систем на рабочих станциях, подключенных к сети Интернет.

16.2. Принципы антивирусного контроля:

1) антивирусное программное обеспечение настраивается на автоматический запуск при включении сервера или рабочей станции;

2) не допускается останавливать процесс сканирования вирусов, кроме случаев, когда требуется установка или решение иной задачи администрирования по согласованию с подразделениями информационной безопасности;

3) обновление антивирусного программного обеспечения и базы данных сигнатур необходимо осуществлять регулярно;

4) нормы сканирования вирусов (например, периодичность, сканируемая область диска, исключение из процесса сканирования и так далее) не допускается изменять настройки конфигурации антивирусного приложения без предварительного согласия отдела информационных технологии и отдела информационной безопасности;

5) файл, полученный из внешних источников (приложения к электронным письмам, съемные носители) необходимо сканировать в момент первого доступа, как на стороне сервера, так и на стороне рабочей станции;

6) об отклонениях в работе антивирусного программного обеспечения необходимо информировать отдел информационной безопасности;

7) файлы регистрации, сгенерированные антивирусным программным обеспечением, подлежат регулярной оценке отделом информационной безопасности.

16.3. Детальная формулировка требований содержится в Правилах организации антивирусного контроля.

17. ИСПОЛЬЗОВАНИЕ МОБИЛЬНЫХ УСТРОЙСТВ И СЪЕМНЫХ НОСИТЕЛЕЙ

17.1. Согласно постановлению Правительства Республики Казахстан от 14 сентября 2004 года № 965 «О некоторых мерах по обеспечению информационной безопасности в Республике Казахстан» в целях обеспечения информационной безопасности установлено, что размещение технических средств, подключенных к международным (глобальным) сетям передачи данных, сети Интернет и/или к информационным сетям, сетям связи, имеющим выход в международные (глобальные) сети передачи данных, сеть Интернет осуществляется вне помещений, выделенных для проведения совещаний (переговоров), в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственные секреты.

17.2. Не допускается использование, внос мобильных устройств, имеющих функцию записи аудио и видеофайлов, в помещения, где используется, циркулирует, хранится служебная и государственная тайна.

Съемные носители, содержащие служебную, конфиденциальную информацию, необходимо регистрировать и маркировать, как указано в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации;

Служебные съемные носители секретной, служебной и конфиденциальной информации необходимо регистрировать в отделе по защите государственных секретов.

Хранение служебных съемных носителей информации осуществляется в защищенных сейфах или металлических шкафах с контролем доступа (опечатывающим устройством).

Утеря служебного съемного носителя и мобильного устройства с хранящейся секретной, служебной и конфиденциальной информацией расценивается как инцидент в системе безопасности и подлежит расследованию.

18. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

18.1. Для обеспечения информационной безопасности необходимо физически предотвратить и ограничить несанкционированный доступ лиц в помещения организаций и учреждений, к оборудованию, информационным системам Университета.

18.2. Физическая безопасность обеспечивается:

1) непрерывной охраной объектов обработки и хранения информации по периметру, как вокруг зданий, так внутри помещений с оборудованием, с установкой необходимых систем защиты от вторжения;

2) ограничением доступа в помещения обработки и хранения информации лицам, не имеющим соответствующего допуска;

3) защитой помещений от внешних угроз чрезвычайных ситуации природного и техногенного характера;

4) системами электроснабжения, водоснабжения, кондиционирования воздуха для бесперебойной работы оборудования обработки и хранения информации в соответствии с требуемыми условиями эксплуатации;

5) регулярным техническим обслуживанием оборудования обработки и хранения информации с привлечением соответствующего обслуживающего персонала, с ограничением доступа к засекреченной информации с соблюдением требований по защите государственных секретов;

6) вывозом и выносом оборудования обработки и хранения информации за пределы организации при наличии соответствующего письменного разрешения руководства Университета;

7) списанием неиспользуемого оборудования правовым актом руководства Университета при условии безопасного удаления всей хранящейся на оборудовании информации.

18.3. Детальная формулировка требований содержится в Правилах организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов.

19. РУКОВОДСТВО ДЛЯ АДМИНИСТРАТОРОВ, УПРАВЛЕНИЕ КОММУНИКАЦИЯМИ И ОПЕРАЦИОННОЙ ДЕЯТЕЛЬНОСТЬЮ

19.1. Управление бизнес-приложениями и системами инфраструктуры осуществляется назначенными администраторами, которые в своей деятельности руководствуются документальными процедурами, обновляемыми в случае изменения приложений или компонентов оборудования.

19.2. Принципы деятельности администратора:

1) устанавливается разделение обязанностей для снижения риска злоупотреблений (включение положений о согласовании и контроле в рабочие процедуры, которые осуществляются персоналом, не имеющим зависимости от персонала, выполняющего процедуру);

2) Департамент цифровизации и автоматизации процессов и руководство Университета обеспечивают владение администраторами необходимыми навыками для поддержки информационных систем, баз данных и прочих компонентов инфраструктуры;

3) отдел информационной безопасности поддерживает необходимый уровень знаний по вопросам безопасности среди администраторов;

4) администраторы осведомляются о текущих вопросах безопасности поддерживаемых систем;

5) уровень доступа администратора к операционным системам и прочим компонентам предоставляется только администратору;

6) возникающие проблемы разрешаются только соответствующими администраторами (при планировании вмешательства администратор обеспечивает максимально короткое время отсутствия доступа к системе или приложению);

7) администраторы выполняют особые поручения при возникновении внештатных ситуаций, которые описываются в соответствующих планах по обеспечению непрерывности операционной деятельности;

8) администраторы отвечают за планирование и осуществление периодического технического обслуживания в соответствии с требованиями производителя, с целью предотвращения сбоев оборудования. По возможности техническое обслуживание осуществляется администратором.

19.3. В период технического обслуживания необходимо выполнить следующие требования:

1) обеспечить доступность данных, хранящихся в системе, только для авторизованного персонала;

2) не допускать нарушения безопасности (кражи, исчезновения или некорректной работы) при предоставлении физического доступа к оборудованию;

3) возложить на администраторов ответственность за установку последних обновлений, патчей (файлы правки, заплатки) на рабочих станциях;

4) возложить на администраторов ответственность за отслеживание и планирование распределения ёмкости компонентов и за запуск процессов увеличения ёмкости;

5) внедрить средства управления безопасностью сети и регистрацию деятельности сети.

19.4. Детальная формулировка требований содержится в Руководстве администратора по сопровождению объекта информатизации и Правилах по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

20. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ

20.1. При эксплуатации информационных систем обеспечивается резервное копирование и контроль за своевременной актуализацией электронных информационных ресурсов.

Для обеспечения доступности и отказоустойчивости собственниками и владельцами информационных систем обеспечивается наличие резервного собственного или арендованного серверного помещения для объектов информатизации «электронного правительства» первого и второго классов в соответствии с классификатором.

20.2. Принципы резервного копирования и восстановления данных информационных систем:

1) процедуры резервного копирования и восстановления данных обеспечивают целостность данных и защиту от утери информации в течение более долгого периода чем тот, который обозначен как «окно уязвимости» в деловой среде, пользующейся информацией;

2) в соответствии с требованиями бизнес-процессов планируется периодичность, график и тип резервных копий;

3) емкость оборудования резервного копирования и хранения данных готовятся в соответствии с ожиданиями в отношении объема данных;

4) оборудование резервного копирования подлежит регулярным испытаниям, а резервные копии необходимо тестировать после создания на предмет целостности и возможности восстановления содержащейся в них информации;

5) резервные копии хранятся в защищенном месте, на достаточном физическом расстоянии от исходных систем с целью недопущения разрушения или повреждения информации на оригинальных и резервных источниках при одном событии;

6) резервные копии подлежат маркировке для определения их типа, даты создания, содержания и степень конфиденциальности информации;

7) процедуры резервного копирования данных определяют срок их хранения и периодичность полного и инкрементного копирования;

8) процедуры резервного копирования максимально автоматизируются, создание резервных копий надлежащим образом документируется Технической службой;

9) процедуры резервного копирования испытываются на предмет восстановления информации из резервных копий;

10) процедура восстановления данных заблаговременно планируется и документируется с указанием порядка восстановления данных из резервных копий;

11) при восстановлении данных из резервных копий необходимо соблюдать требования безопасности для предотвращения несанкционированного доступа к восстановленным данным;

12) неиспользуемые носители резервных копий подлежат сбору, хранению и гарантированному уничтожению с составлением акта в присутствии подразделения информационной безопасности и с исключением возможности восстановления содержащейся на них информации Технической службой.

20.3. Детальная формулировка требований содержится в Регламенте резервного копирования и восстановления информации и Правилах по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

21. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

21.1. Инциденты и внештатные (кризисные) ситуации в системе информационной безопасности подлежат регистрации и расследованию отделом информационной безопасности совместно с Департаментом цифровизации и автоматизации процессов при этом необходимо обеспечить своевременность предпринимаемых действий.

21.2. Принципы управления инцидентами:

1) создаются соответствующие каналы коммуникации, позволяющие получить доступ к сообщениям о различных инцидентах и внештатных (кризисных) ситуациях в системе безопасности от Департамента цифровизации и автоматизации процессов;

2) пользователи и Департамент цифровизации и автоматизации процессов обязаны сообщать о замеченных или предполагаемых инцидентах в системе безопасности, включая утечку конфиденциальной информации, вредоносные атаки, замеченные или предполагаемые уязвимые места в системе безопасности, отсутствие доступа или некорректная работа оборудования;

3) отделом информационной безопасности или иным назначенным лицам необходимо вести журналирование событий информационной безопасности;

4) сообщения об инцидентах регистрируются подразделениями информационной безопасности или иными назначенными лицам с последующим расследованием;

5) отдел информационной безопасности обязан сообщать об инцидентах руководству при высокой степени тяжести инцидента;

6) исходя из результатов оперативного анализа инцидента руководством принимается решение о принятии мер по внештатной (кризисной) ситуации;

7) мероприятия по реагированию на внештатные (кризисные) ситуации заблаговременно планируются и оформляются документально для минимизации дальнейшего ущерба и восстановления нормативного функционирования оборудования и информационных систем Университета в предварительно определенные сроки;

8) в случае если инцидент имеет значительное негативное воздействие на функционирование оборудования и информационных систем Университета, необходимо уведомить подразделение информационной безопасности Университета.

21.3. При анализе инцидентов подразделениями информационной безопасности рассматриваются следующие параметры:

- каким образом инцидент был обнаружен;
- вследствие какой уязвимости произошел инцидент;
- последствия инцидента;
- принятые меры по минимизации ущерба;
- как принятые меры по минимизации ущерба предотвратят повторение инцидента;
- обнаружены ли по процедуре прочие уязвимости или инциденты, которые необходимо исследовать;
- как снизить риск подобных инцидентов.

Инциденты в системе информационной безопасности оцениваются ежегодно (совместно с Оценкой и анализом рисков), по результатам оценки даются рекомендации по снижению риска происшествий в будущем.

Согласно Единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденным постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832, при выявлении аномальной активности и злоумышленных действий пользователей информируются подразделения информационной безопасности, техническая служба реагирования на инциденты информационной безопасности.

21.4. Детальная формулировка требований содержится в Правилах по обеспечению непрерывной работы активов, связанных со средствами обработки информации и Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях.

22. БЕЗОПАСНОСТЬ ЧЕЛОВЕЧЕСКИХ РЕСУРСОВ

22.1. Человеческие ресурсы, имеющие доступ к рабочим станциям и информационным система Университета, в качестве пользователей, операторов или третьих лиц, ознакамливаются с Политикой и придерживаются её.

22.2. Функциональные обязанности по обеспечению информационной безопасности и обязательства по исполнению требований технической документации по информационной безопасности вносятся в должностные инструкции и (или) условия трудового договора.

22.3. В зависимости от информации с которой предстоит ознакомиться сотрудник или работник Университета до начала исполнения должностных обязанностей проходит процедуру допуска к секретной, служебной и конфиденциальной информаций в соответствии с действующим законодательством.

22.4. Кадровая служба Университета организует и ведет учет прохождения служащими или работниками организаций обучения в сфере информатизации и области обеспечения информационной безопасности.

22.5. Соблюдение сотрудниками и работниками требований информационной безопасности контролируется Отделом информационной безопасности.

23. ПРИОБРЕТЕНИЕ, РАЗРАБОТКА И ПОДДЕРЖКА ИНФОРМАЦИОННЫХ СИСТЕМ

23.1. Оборудование (рабочие станции) и информационные системы Университета вводятся в работу исключительно под контролем, с учетом всех аспектов информационной безопасности.

23.2. Принципы приобретения, разработки и поддержки информационных систем:

1) согласование конкурсной документации для закупки элементов аппаратного или программного обеспечения информационных систем Университета с руководителем департамента цифровизации и автоматизации процессов;

2) по согласованию с отделом информационной безопасности в техническую спецификацию конкурсной документации для закупки элементов аппаратного или программного обеспечения информационных систем Университета вносятся требования информационной безопасности в соответствии с нормативными правовыми актами и стандартами;

3) перед началом опытной эксплуатации информационной системы для всех функциональных компонентов информационный системы создается набор тестов, сценариев тестирования и методика испытаний для проведения тестирования, осуществляются стендовые испытания информационной системы и обучение персонала;

4) информационные системы подлежат испытанию на соответствие требованиям информационной безопасности;

5) ввод в промышленную эксплуатацию информационных систем осуществляется в соответствии с требованиями технической документации при условии положительного завершения опытной эксплуатации, наличия акта с положительным результатом испытаний на соответствие требованиям информационной безопасности и подписания акта о вводе в промышленную эксплуатацию информационной системы приемочной комиссией с участием представителей уполномоченного органа в области информационной безопасности, заинтересованных органов и организаций;

6) объекты информатизации электронного правительства первого и второго классов в соответствии с классификатором подключаются к системе мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования не позднее одного года после их введения в промышленную эксплуатацию.

23.3. При промышленной эксплуатации информационных систем обеспечиваются:

1) сохранность, защита, восстановление электронных информационных ресурсов в случае сбоя или повреждения;

2) резервное копирование и контроль за своевременной актуализацией электронных информационных ресурсов;

3) автоматизированный учет, сохранность и периодическое архивирование сведений об обращениях к информационной системе;

4) мониторинг событий информационной безопасности информационных систем и передача его результатов в систему мониторинга обеспечения информационной безопасности государственной технической службы;

5) фиксация изменений в конфигурационных настройках программного обеспечения, серверного и телекоммуникационного оборудования;

6) контроль и регулирование функциональных характеристик производительности;

7) сопровождение информационных систем;

8) техническая поддержка используемого лицензионного программного обеспечения;

9) гарантийное обслуживание разработчиком информационных систем, включающее устранение ошибок и недочетов, выявленных в период гарантийного срока. Гарантийное обслуживание обеспечивается сроком не менее года со дня введения в промышленную эксплуатацию информационной системы;

10) подключение пользователей к информационной системе, а также взаимодействие информационной системы осуществляется с использованием доменных имен.

24. СОБЛЮДЕНИЕ НОРМ ЗАКОНОДАТЕЛЬСТВА

24.1. Функционирование оборудования и информационных систем Университета осуществляется в соответствии с требованиями законов и норм Республики Казахстан, а также внутренних норм Университета.

24.2. В соответствии со статьёй 138 Предпринимательского Кодекса Республики Казахстан в сфере информатизации в части обеспечения информационной безопасности осуществляется государственный контроль Комитетом по информационной безопасности Министерства цифрового развития, инновации и аэрокосмической промышленности Республики Казахстан.

Контроль осуществляется согласно норм Критериев оценки степени риска и проверочных листов в сфере информатизации в части обеспечения информационной безопасности, утвержденных совместным приказом заместителя Премьер-Министра Республики Казахстан - Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года № 12.

25. НАРУШЕНИЕ ТРЕБОВАНИЙ ПОЛИТИКИ

25.1. Ответственность за соблюдение Политики возлагается на собственников, владельцев и пользователей информационных систем Университета в пределах компетенции. Неисполнение требовании Политики влечет привлечение к дисциплинарной ответственности, в случае отсутствия состава административного и уголовного правонарушения, в соответствии с действующим законодательством Республики Казахстан.

25.2. Нарушение Политики расценивается как инцидент в системе безопасности и подлежит расследованию.

25.3. В ходе расследования в каждом отдельном случае руководство Университета определяет меру дисциплинарного взыскания за нарушение требований Политики.

25.4. Инциденты расследуются отделом информационной безопасности Университета.

25.5. Результаты расследования оформляются документально с указанием следующих деталей:

1) выявленное событие, в результате которого произошел инцидент в системе безопасности;

2) обстоятельства и лицо, выявившее событие;

3) нарушенная норма правил и последствия такого нарушения;

4) рекомендации и предложения для предупреждения возникновения аналогичных инцидентов.