ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТ - 2023

СОДЕРЖАНИЕ

1. Введение

Университет общественной безопасности Республики Узбекистан (далее – Университет) был сформирован на основании Постановления Президента Республики Узбекистан от 15 апреля 2021 года № ПП-5077 «О мерах по дальнейшему совершенствованию системы подготовки профессиональных кадров в сфере обеспечения общественной безопасности». Университет входит в систему Национальной гвардии Республики Узбекистан (далее – НГ РУ) как образовательное учреждение, способствующее более качественному выполнению возложенных на Национальную гвардию задач. Университет является базовым высшим военным образовательным и научно-исследовательским учреждением, осуществляющим целевую подготовку квалифицированных кадров.

Основными задачами и направлениями деятельности Университета являются:

целевая подготовка квалифицированных специалистов, способных эффективно организовать деятельность по обеспечению общественной безопасности, посредством углубленного обучения по соответствующим профильным и правовым направлениям, осуществления их боевой и физической подготовки;

углубленная подготовка кадров для Вооруженных Сил и правоохранительных органов путем внедрения эффективной системы духовно-нравственного воспитания, формирования у них правовой культуры, патриотических и высоких морально-нравственных качеств;

переподготовка и повышение квалификации воспитателей учебно-воспитательных учреждений в направлении военного патриотизма, духовно-просветительского воспитания и общественной работы с молодежью;

организация учебного процесса путем обеспечения взаимосвязи теории и практики с применением современных форм и методов преподавания, педагогических и информационных технологий;

подготовка научно-педагогических кадров высшей квалификации, проведение комплексных научных исследований по наиболее актуальным проблемам обеспечения общественной безопасности, в том числе с привлечением отечественных и международных грантов;

привлечение к учебному процессу квалифицированных специалистов ведущих образовательных и научно-исследовательских учреждений зарубежных государств, а также постоянное осуществление международного сотрудничества в области проведения совместных научных исследований и обмена педагогическим опытом.

Для реализации своих задач и функций Университет широко внедряет в свою деятельность современные информационно-коммуникационные технологии (далее - ИКТ). Внедрение ИКТ в Университете должно сопровождаться решением задач обеспечения информационной безопасности.

Информационная безопасность рассматривается с позиции сохранения конфиденциальности, целостности и доступности информации, а также обеспечения непрерывного и бесперебойного функционирования эксплуатируемых и внедряемых информационных систем и ресурсов Университета. Информационная безопасность достигается путем внедрения и реализации комплекса мер, включающих в себя политики, технические средства, программное обеспечение, практику, процедуры и организационные структуры. Комплекс мер по информационной безопасности должен обеспечивать защиту информации (данных) Университета и поддерживающую её информационно-коммуникационную инфраструктуру от широкого спектра угроз, с целью обеспечения непрерывной деятельности Университета, минимизации ущерба от реализации угроз, прогнозирования и предотвращения их воздействия, поддержания деловой репутации и соблюдения требований законодательства.

Политика информационной безопасности Университета определяет основные принципы по защите его информационных активов и информационно-коммуникационной инфраструктуры. Она служит основой для принятия соответствующих документов по управлению и построению системы управления информационной безопасностью (далее - СУИБ) в Университете. Настоящая Политика информационной безопасности представляет собой совокупность документированных руководящих принципов, правил, процедур и практических методов, и средств в области информационной безопасности, которыми Университет руководствуется в своей деятельности.

Настоящая Политика согласована с ГУП «Центр кибербезопасности» при Службе государственной безопасности Республики Узбекистан (письмо №_____ от _____202__ г.), Министерством цифровых технологий Республики Узбекистан (письмо №_____от _____202__ г.) и со Службой государственной безопасности Республики Узбекистан (письмо №_____от _____ 202__ г.).

2. Нормативные ссылки

2.1. Политика информационной безопасности разработана в соответствии с нижеследующими документами по обеспечению информационной безопасности объектов информатизации Республики Узбекистан:

2.1.1. Закон Республики Узбекистан от 11 декабря 2003 года, № 560-П «Об информатизации».

2.1.2. Закон Республики Узбекистан от 11 декабря 2003 года № 562-II «Об электронной цифровой подписи».

2.1.3. Закон Республики Узбекистан от 29 апреля 2004 года № 611-II «Об электронном документообороте».

2.1.4. Закон Республики Узбекистан от 11 сентября 2014 года №374 «О коммерческой тайне».

2.1.5. Закон Республики Узбекистан от 9 декабря 2015 года №395 «Об электронном правительстве».

2.1.6. Закон Республики Узбекистан от 2 июля 2019 года №ЗРУ-547 «О персональных данных».

2.1.7. Закон Республики Узбекистан от 11 ноября 2020 года № ЗРУ-647 «О Национальной гвардии Республики Узбекистан».

2.1.8. Закон Республики Узбекистан от 15 апреля 2022 года №ЗРУ-764 «О кибербезопасности».

2.1.9. Указ Президента Республики Узбекистан от 15 июня 2020 года №УП-6007 «О мерах по внедрению Государственной системы защиты информационных систем и ресурсов Республики Узбекистан».

2.1.10. Постановление Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан».

2.1.11. Постановление Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов».

2.1.12. Постановление Президента Республики Узбекистан от 15 июня 2020 года №ПП-4751 «О мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан».

2.1.13. Постановление Президента Республики Узбекистан от31 мая 2023 года №ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан».

2.1.14. Постановление Кабинета Министров Республики Узбекистан от 22 ноября 2005 года № 256 «О совершенствовании нормативно-правовой базы в сфере информатизации».

2.1.15. Постановление Кабинета Министров Республики Узбекистан от 4 мая 2011 года № 126 «О мерах по внедрению и использованию единой защищенной электронной почты и системы электронного документооборота в исполнительном аппарате Кабинета Министров, органах государственного и хозяйственного управления, государственной власти на местах».

2.1.16. Постановление Кабинета Министров Республики Узбекистан от 14 июня 2013 года №170 «О дополнительных мерах по дальнейшему совершенствованию системы аттестации объектов информатизации».

2.1.17. Постановление Кабинета Министров Республики Узбекистан от 7 ноября 2011 года №296 «О мерах по реализации постановления от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов».

2.1.18. Постановление Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан».

2.1.19. O‘zDSt ISO/IEC 27000:2022 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь».

2.1.20. O‘zDSt ISO/IEC 27001:2020 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования».

2.1.21. O‘zDSt ISO/IEC 27002:2016 «Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасности».

2.1.22. O‘zDSt ISO/IEC 27003:2022 «Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью».

2.1.23. O‘zDSt ISO/IEC 27005:2013 «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности».

2.1.24. O‘zDStISO/IEC 27007:2022 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью».

2.1.25. O‘zDSt ISO/IEC 27008:2022 «Информационная технология. Методы обеспечения безопасности. Руководство для аудиторов по средствам управления информационной безопасностью».

2.1.26. O‘zDSt ISO/IEC 27010:2015 «Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и между организациями».

2.1.27. O‘zDSt ISO/IEC 27014:2018 «Информационная технология. Методы обеспечения безопасности. Корпоративное управление информационной безопасностью».

2.1.28. O‘zDSt ISO/IEC 27031:2016 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».

2.1.29. O‘zDSt ISO/IEC 27032:2017 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по кибербезопасности».

2.1.30. O‘zDSt ISO/IEC 27033-1:2016 «Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции».

2.1.31. O‘zDSt ISO/IEC 27033-4:2016 «Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности».

2.1.32. O‘zDSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами».

2.1.33. O‘zDSt 3387:2019 (ISO/IEC 27035-2:2016, MOD) «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Руководящие указания по планированию и подготовке к реагированию на инциденты».

2.1.34. O‘zDSt 1047:2018 «Информационная технология. Термины и определения».

2.1.35. O‘zDSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения.

2.1.36. O‘zDSt 1109:2013 «Информационная технология. Криптографическая защита информации. Термины и определения».

2.1.37. O‘zDSt ISO/IEC 15408-1:2016 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

2.1.38. O‘zDSt ISO/IEC 15408-2:2016 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».

2.1.39. O‘zDSt ISO/IEC 15408-3:2016 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

2.1.40. O‘zDSt ISO/IEC 13335-1:2009 «Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий (часть 1). Концепции и модели управления безопасностью информационно-коммуникационных технологий».

2.1.41. O‘zDSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации».

2.1.42. O‘zDSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации».

2.1.43. O‘zDSt 2816:2014 «Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей».

2.1.44. O‘zDSt 2817:2014 «Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации».

2.1.45. O‘zDSt2875:2014 «Требования к дата-центрам. Обеспечение инфраструктуры и информационной безопасности».

2.1.46. RH 45-015:2016 «Унифицированные системы документации. Организационно-распорядительная документация. Виды, состав и оформление».

2.1.47. Инструкция о порядке учета, обращения и хранения документов, дел и изданий, содержащих несекретные сведения ограниченного распространения, утвержденная 5 декабря 2006 года заместителем Премьер-министра Республики Узбекистан – председателем межведомственной комиссии по вопросам защиты государственных секретов.

2.1.48. Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан (Приложение №10 к протоколу Республиканской комиссии по координации реализации Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на 2013-2020 годы от 23 февраля 2016 года № 7).

2.1.49. Регламент взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию, расследованию и предотвращению инцидентов информационной безопасности (приложение №1 к протоколу Технического совета по вопросам информационно-коммуникационной безопасности Республики Узбекистан от 17.11.2017г. №7).

2.1.50. Требования обеспечения информационной безопасности органов государственного и хозяйственного управления, государственной власти на местах (Приложение №2 к протоколу Технического совета по вопросам информационно-коммуникационной безопасности Республики Узбекистан от 17.11.2017г. №7).

3. Термины и определения

3.1. В настоящем документе применены термины согласно государственному стандарту O‘zDSt 2927:2015 «Информационная безопасность. Термины и определения». Также в тексте встречаются термины с соответствующими определениями:

3.1.1. **Анализ рисков:** систематическое выполнение процедур идентификации ресурсов системы обработки данных, угроз этим ресурсам и уязвимостей системы к этим угрозам.

3.1.2. **База данных:** совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ.

3.1.3. **Безопасность информации:** состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

3.1.4. **Документированная информация:** зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

3.1.5. **Нарушитель (злоумышленник):** лицо или организация, заинтересованные в получении несанкционированного доступа к информационной системе и ее ресурсам и совершившие преднамеренные действия для их несанкционированного получения или изменения.

3.1.6. **Информационный ресурс:** отдельные документы, отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других).

3.1.7. **Информационная система:** организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией.

3.1.8. **Информация ограниченного доступа:** документированная информация, содержащая сведения, составляющие государственные секреты и конфиденциальную информацию, доступ к которой ограничивается в соответствии законодательством.

3.1.9. **Инцидент информационной безопасности:** единичное событие или ряд нежелательных, или непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации защищаемой информации и реализации угрозы информационной безопасности.

3.1.10. **Конфиденциальная информация:** документированная информация, не содержащая сведений, составляющих государственные секреты, доступ к которой ограничивается в соответствии с законодательством.

3.1.11. **Несанкционированный доступ:** доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.

3.1.12. **Объект информатизации:** информационные системы различного уровня и назначения, сети телекоммуникаций, технические средства обработки

информации, помещения, где установлены и эксплуатируются эти средства, а также отдельные помещения, предназначенные для ведения переговоров в т.ч, конфиденциальные.

3.1.13. **Оценка рисков:** процесс сравнения рассчитанного риска и критериев риска, выполняемый с целью определения его значения.

3.1.14. **Персональные данные:** сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

3.1.15. **Пользователи:** военнослужащие, сотрудники и служащие подразделений Университета (далее - сотрудники), которым предоставлен доступ к корпоративной сети и информационным ресурсам, а также доступ к сети Интернет.

3.1.16. **Программное обеспечение:** совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

3.1.17. **Риск:** возможность использования конкретной уязвимости системы обработки данных при реализации конкретной угрозы.

3.1.18. **Сервер:** совокупность аппаратного и программного обеспечения (программа-сервер), позволяющая компьютеру предоставлять услуги другому компьютеру. Компьютеры работают с программой-сервером с помощью программ-клиентов.

3.1.19. **Система управления информационной безопасностью (СУИБ):** часть общей системы управления, основанная на использовании методов оценки бизнес-рисков, предназначенная для разработки, внедрения, функционирования, мониторинга, анализа, обслуживания и совершенствования информационной безопасности.

3.1.20. **Системный администратор:** должностное лицо, назначенное в установленном порядке, ответственное за эксплуатацию службы каталога, систем управления базами данных и прочих систем или серверов, их ведение, настройку, изменение полномочий пользователей, информационную безопасность.

3.1.21. **Средства защиты информации:** технические, криптографические и другие средства, предназначенные для защиты информации, в том числе средства контроля эффективности защиты информации.

3.1.22. **Угроза:** потенциальная возможность нарушения компьютерной безопасности.

3.1.23. **Уязвимость:** недостаток в системе обработки данных, используя который, можно нарушить ее целостность и вызвать неправильную работу.

4. Обозначения и сокращения

4.1. В настоящей Политике применены следующие обозначения и сокращения:

IDPS (IntrusionDetection&Prevention System) – средство обнаружения и предотвращения вторжений;

URL – система унифицированных адресов электронных ресурсов или единообразный определитель местонахождения ресурса;

АВЗ – антивирусная защита;

АИС – автоматизированная информационная система;

АС – автоматизированная система;

БД – база данных;

ДСП – для служебного пользования;

ЗИ – защита информации;

ИБ – информационная безопасность;

ИБП – источник бесперебойного питания;

ИКТ – информационно-коммуникационные технологии;

ИР – информационный ресурс;

ИС –информационная система;

ИТ – информационная технология;

КЗИ – криптографическая защита информации;

КИ – конфиденциальная информация;

ЛВС - локальная вычислительная сеть;

МЭ – межсетевое экранирование;

МЭСП -межсетевой экран следующего поколения;

НСД –несанкционированный доступ;

ОВИТиС - Отдел внедрения информационных технологий и связи ;

ОС –операционная система;

ПО – программное обеспечение;

РС –рабочая станция;

СЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации;

СУБД – система управления базой данных;

СУИБ – система управления информационной безопасностью;

УМСЦ – учебно-методический ситуационный центр;

УС, ИКТиЗИ – Управление связи, информационно-коммуникационных технологий и защиты информации НГ РУ;

ЦОД – центр обработки данных;

СЭД – система электронного документооборота.

5. Область применения

5.1. Настоящая Политика определяет систему планирования и действий подразделения (отдела внедрения информационных технологий и связи – далее ОВИТиС), в вопросе обеспечения информационной безопасности в структуре Университета и представляет собой систематизированное изложение целей и задач защиты, правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Университет в своей деятельности, а также основных принципов построения организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

5.2. Требования настоящей Политики распространяются на все информационные ресурсы и системы Университета за исключением информационных ресурсов и систем, содержащих (обрабатывающих) государственные секреты.

5.3. Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий в Университете, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов защиты Университета.

5.4. Политика информационной безопасности должна использоваться в качестве основы для построения комплексной СУИБ в Университете.

5.5 Основные положения и требования Политики информационной безопасности Университета подлежат исполнению всеми структурными подразделениями Университета, куда входят:

1) Командование;
2) Управление;
3) Отделы;
4) Службы;
5) Центры;
6) Кафедры;
7) Факультеты;
8) Магистратура;
9) Батальоны;
10) Отдельные штатные единицы.

5.6. Университет разрабатывает собственную Политику информационной безопасности, направленную на защиту своих информационных систем и ресурсов, которая согласовывается в установленном порядке и утверждается руководством.

5.7. Требования настоящей Политики распространяются на все информационные системы и ресурсы Университета, на всех военнослужащих, сотрудников, служащих подразделений Университета (далее сотрудники) вне зависимости от их места работы и занимаемой должности, а также на третьих лиц (поставщики, подрядчики, аудиторы, оценщики, посетители, обслуживающий персонал и т.п.), которые по тем или иным причинам имеют легитимный доступ к информационным системам и ресурсам Университета.

5.8. Руководители подразделений Университета должны обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме

того, отдел ВИТиС Университета проводит периодическую проверку соблюдения требований информационной безопасности согласно настоящей Политики с последующим представлением отчета по результатам указанной проверки руководству Университета.

6. Цели и задачи

6.1. Основной целью Политики информационной безопасности Университета является выработка комплексных подходов, принципов, правил, процедур и практических мер, направленных на:

- защиту субъектов информационных отношений от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования объектов информатизации или несанкционированного доступа к циркулирующей в ней информации и её незаконного использования;
- обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности;
- обеспечение работоспособности подсистемы ИБ, а также выполнение требований государственных и иных стандартов в области информационно-коммуникационных технологий и информационной безопасности;
- формирование организационно-методической базы для реализации СУИБ;
- устранение и минимизацию возможных последствий инцидентов информационной безопасности, прогнозирование, предотвращение и пресечение реализации угроз, выявление и устранение уязвимостей на объектах информатизации и СУИБ;
- формирование комплекса организационно-технических мероприятий по обеспечению информационной безопасности и бесперебойного устойчивого функционирования ресурсов и баз данных Университета, с учетом широкого спектра угроз;
- обеспечение резервирования информационных систем и систем восстановления данных;
- обеспечение резервирования систем жизнеобеспечения.

6.2. Основными задачами Политики информационной безопасности являются:

- своевременное выявление и прогнозирование внутренних и внешних угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;
- обеспечение контроля за конфиденциальностью, целостностью и доступностью объектов защиты;
- предотвращение утечки конфиденциальной информации;
- выявление попыток и предотвращение несанкционированного доступа к информационным системам, ресурсам и базам данных Университета, а также съема информации с них;
- классификация ИР и их контроль;

- разработка единых требований, предъявляемых к информационным технологиям, применяемым в сети с точки зрения ИБ;

- определение объектов защиты и их классификация по уровню защищенности в соответствии с государственным стандартом O‘zDSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;

- выявление и устранение уязвимостей в информационно-коммуникационной инфраструктуре и СУИБ Университета;

- сохранение конфиденциальности, целостности и доступности деловой информации Университета, критичных информационных ресурсов, обеспечение работоспособности информационных систем, иных объектов информатизации;

- разработка единых требований, предъявляемых к информационным технологиям, применяемым в информационно-коммуникационной инфраструктуре Университета с точки зрения информационной безопасности;

- создание и развитие СУИБ Университета, обеспечивающей комплексный подход обеспечения информационной безопасности с применением организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации;

- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями пользователей на объектах информатизации;

- подготовка кадров в области защиты информации, повышение осведомленности сотрудников в области рисков информационной безопасности.

7. Основные положения

7.1. Обеспечение информационной безопасности в Университете должно основываться на следующих основных принципах:

- законность – меры по защите информации должны реализовываться с соблюдением Конституции и законодательства Республики Узбекистан, а также требований нормативных актов в области обеспечения информационной безопасности;

- вовлеченность – в процессе обеспечения информационной безопасности должны участвовать руководство и все сотрудники Университета;

- разделение обязанностей - роли и ответственности в вопросах обеспечения информационной безопасности должны четко распределяться между сотрудниками Университета;

- персональная ответственность – сотрудники Университета должны нести персональную ответственность, которая определена в трудовых договорах, должностных инструкциях, а также в договорах (соглашениях) с контрагентами;

- профессионализм – профессиональный уровень знаний сотрудников Университета, ответственных за обеспечение информационной безопасности,

должен постоянно повышаться и применяться в процессах управления информационной безопасностью;

- взаимодействие и согласованность действий - действия по обеспечению информационной безопасности должны осуществляться на основе четкого взаимодействия заинтересованных подразделений и быть согласованными между собой по целям, задачам, принципам, методам и средствам;
- повышенная защищенность - меры обеспечения информационной безопасности должны выбираться с учетом необходимости организации эффективной защиты от всевозможных угроз информационной безопасности;
- системный подход - при построении СУИБ должны учитываться все взаимосвязанные, взаимодействующие и изменяющиеся во времени элементы, условия и факторы, значимые для понимания и решения проблемы обеспечения информационной безопасности;
- комплексность – должны использоваться разнородные методы и средства защиты, которые в совокупности организовывают целостную систему защиты, не содержащую слабых мест и обеспечивающую эшелонированную защиту всех защищаемых объектов;
- непрерывность защиты – процесс обеспечения информационной безопасности должен быть постоянным по времени и идти на всех уровнях Университета;
- подконтрольность и учет действий – выполнение принятых требований информационной безопасности сотрудниками должны контролироваться и учитываться все действия их в информационных системах Университета;

7.2. Применяемые в Университете меры и методы информационной безопасности (приведены в разделе 11 настоящей Политики) должны быть направлены на:

- обнаружение, предотвращение и предупреждение угроз информационной безопасности;
- устранение уязвимостей и недостатков в системе защиты информации Университета;
- оперативное реагирование на возникшие инциденты информационной безопасности;
- обеспечение живучести информационных систем на случай реализации угроз информационной безопасности;
- локализацию угроз информационной безопасности и ликвидацию последствий от их реализации с восстановлением нормального функционирования информационных систем Университета.

7.3. Информационная безопасность в Университете должна обеспечиваться с использованием совокупности правовых, организационных, технических и других методов и мер защиты информации, а также за счет всестороннего непрерывного контроля эффективности реализованных мер информационной безопасности.

8. Объекты защиты

8.1. Объектами защиты от угроз информационной безопасности Университета являются:

1) конфиденциальная документированная информация в бумажном и электронном виде включая:

- служебная информация Университета;
- конфиденциальная информация сторонних организаций (поставщики, заказчики, партнеры, подведомственные организации и др.);
- конфиденциальная информация, обмениваемая с государственными органами и организациями;
- персональные данные сотрудников Университета.

2) сотрудники Университета, являющиеся разработчиками информационных систем Университета;

3) рабочие станции, сервера, хранилища данных и иные средства обработки и хранения информации;

4) операционные системы, прикладное программное обеспечение и приложения, СУБД;

5) корпоративная сеть передачи данных Университета, ЛВС объектов Университета, каналы передачи данных, сетевые кабели, сетевое оборудование (маршрутизаторы, таблицы маршрутизации, управляемые и неуправляемые коммутаторы);

6) система корпоративной электронной почты Университета;

7) информационные ресурсы: официальный веб-сайт Университета, файловые хранилища и базы данных информационных систем Университета;

8) носители защищаемой информации, в том числе носители конфиденциальной информации;

9) серверное помещение Университета, в котором размещается серверное оборудование, сетевое телекоммуникационное оборудование и средства защиты информации, а также помещения, в которых осуществляется обработка конфиденциальной информации;

10) средства защиты информации (межсетевые экраны, средство IDPS, антивирусы, СКЗИ и др.);

11) нематериальные активы (репутация и имидж Университета).

8.2. Основными объектами информатизации Университета, подлежащими обеспечению информационной безопасности, являются:

1) корпоративная сеть передачи данных Университета;

2) ЛВС Университета и его подразделений, указанных в пункте 5.5 настоящей Политики;

3) официальный веб-сайт Университета - https://mgjxu.uz (информационная безопасность данного ресурса обеспечивается подрядной организацией – ООО “ЕИ Uzinfocom” согласно заключенного договора);

4) файловые хранилища информации объектов Университета;

5) корпоративная электронная почта https://corp.uz (информационная безопасность данного ресурса обеспечивается подрядной организацией – ООО “ЕИ Uzinfocom” согласно заключенного договора);

6) информационные системы и входящие в них базы данных Университета:

- система видеоконференцсвязи Университета (Vinteo);
- электронная библиотека Университета.

7) серверное помещение, размещенное в учебно-методическом ситуационном Центре (далее - УМСЦ) Университета (здание на территории Университета, адрес: Ташкентская область, Зангиатинский район, посёлок Чорсу), включающее в себя:

- серверную комнату (помещение 115), в которой размещаются серверное оборудование информационных систем и ресурсов Университета, основное сетевое оборудование;
- кроссовое помещение.

8) Помещение для проведения переговоров и совещаний руководства (здание учебного корпуса, блок «А», 4 этаж, аудитория каф. ТСП, адрес: Ташкентская область, Зангиотинский район, посёлок Чорсу),.

8.3. Классификация по уровню защищенности информационных ресурсов Университета приведена в Реестре информационных ресурсов Университета согласно приложению №15 к настоящей Политике.

8.4. Классификация по уровню защищенности информационных систем Университета осуществлена в соответствии с Требованиями обеспечения информационной безопасности органов государственного и хозяйственного управления, государственной власти на местах (Приложение №2 к протоколу Технического совета по вопросам информационно-коммуникационной безопасности Республики Узбекистан от 17.11.2017г. №7) и приведена в таблице №1.

Таблица №1. Классификация по уровню защищенности информационных систем Университета

Наименование ИС	**Масштаб ИС**	**Категория обрабатываемой информации**	**Уровень значимости ИС**	**Класс защищенности ИС***
Система видеоконференц связи	Университет	открытая	средний	второй класс ИС2

*Примечание: Самым низким классом защищенности принят первый класс (ИС1), а самым высоким – четвертый класс (ИС4).

9. Риск и модель угроз информационной безопасности

9.1. Угрозы информационной безопасности Университета направлены на нарушение конфиденциальности, целостности и доступности его информации, а также на нарушение нормального бесперебойного функционирования объектов информатизации Университета.

9.2. Угрозы информационной безопасности Университета по природе их возникновения могут быть естественные (объективные) и искусственные (субъективные).

Источники угроз информационной безопасности могут быть внутренними (источник угроз внутри Университета) и внешними (источник угроз вне Университета).

9.3. По способу воздействия основными угрозами информационной безопасности Университета являются:

- компьютерно-технические угрозы;
- физические угрозы;
- угрозы с использованием технических каналов утечки информации;
- техногенные угрозы, включая угрозы природного характера;
- организационные и правовые (юридические) угрозы.

Компьютерно-технические угрозы реализуются посредством сетевого взаимодействия на объект защиты и/или с использованием программ, компьютерных средств, а также уязвимостей в них.

Компьютерные угрозы по характеру воздействия делятся на:

- информационные – распространение нежелательной, недостоверной, противоречащей деятельности Университета информации в электронном виде;
- программные – вредоносные программы, использование специализированных программ или не декларированных функциональных возможностей (закладок) в программах;
- сетевые – сетевые атаки и воздействия, использование уязвимостей в сети и сетевых протоколах, использование каналов передачи информации и уязвимостей в программах.
- отказы в обслуживании технических и программных средств.

Физические угрозы реализуются посредством физического несанкционированного доступа в помещения организации, в кабинеты и серверную комнату, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и иных объектов защиты. Кража или повреждение компьютерного оборудования и носителей информации инсайдерами.

Угрозы с использованием технического канала утечки информации реализуются посредством прослушивания физического пути сигнала от источника передачи данных к приемному устройству злоумышленника. Сам процесс односторонний, и с его помощью человек не санкционированно получает скрытые сведения или личную информацию, которую можно зафиксировать.

Техногенные угрозы, включая угрозы природного характера:

возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, необусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, необусловленных напрямую деятельностью человека.

К *организационно-правовым угрозам* относятся:

закупки несовершенных или устаревших информационных технологий и средств информатизации;

нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере.

9.4. Для определения актуальности угроз информационной безопасности используются два критерия:

- опасность угрозы;
- возможность возникновения и реализации угрозы.

Опасность угрозы оценивается, исходя из последствий, которые возникнут в результате реализации угрозы, и имеет значения:

- высокая – сильные последствия;
- средняя – умеренные последствия;
- низкая – незначительные последствия.

Возможность возникновения и реализации угрозы имеет следующие значения:

- высокая - наличие уязвимости и отсутствие методов и средств защиты от угрозы, распространённость угрозы в информационном пространстве;
- средняя - наличие уязвимости в программном обеспечении, применение менее эффективных методов и средств защиты информации, угроза не имеет широкого распространения в информационном пространстве;
- низкая – отсутствие уязвимости, использование средств защиты, реализация угрозы имеет конкретный характер.

Актуальность угрозы информационной безопасности определяется по правилам, приведенным в таблице №2.

Таблица №2. Правила определения актуальности угроз информационной безопасности

Возможность реализации угрозы	Опасность угрозы		
	Низкая	Средняя	Высокая
Низкая	-	-	актуальная
Средняя	-	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

9.5. Модель угроз информационной безопасности Университета

определяется в отношении объектов защиты и включает в себя:

- описание угрозы;
- источник и природу угрозы;
- способ реализации угроз;
- используемые уязвимости;
- объекты воздействия;
- актуальность угрозы (опасность и возможность реализации);

Модель основных угроз информационной безопасности Университета приведена в таблице №3.

9.6. В целях определения уровня обеспечения информационной безопасности Университета ОВИТиС проводится анализ и оценка рисков. Риски определяются вероятностью причинения ущерба и потерь в случае реализации угроз информационной безопасности.

9.7. Анализ и оценка рисков в Университете проводится в соответствии с государственным стандартом O‘zDSt ISO/IEC 27005:2013 «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности».

9.8. При анализе рисков учитываются только актуальные угрозы информационной безопасности.

Анализ рисков и угроз информационной безопасности в отношении объектов защиты приведен в таблице №4.

Для снижения рисков информационной безопасности при взаимодействии со сторонними организациями должны реализовываться меры безопасности в отношениях с внешними пользователями, которые приведены в разделе 11 настоящей Политики.

9.9. Процесс управления рисками информационной безопасности включает в себя не только анализ и оценку рисков, но и меры, направленные на снижение рисков информационной безопасности.

Указанные меры должны применяться в отношении рисков с уровнем «выше среднего» и «высокая». Данные меры определяются ОВИТиС и согласовываются с руководством Университета.

9.10. Результаты мер, принятых для управления рисками информационной безопасности, должны документироваться и их выполнение контролироваться начальником ОВИТиС.

Таблица №3. Модель основных угроз информационной безопасности Университета

Наименование угрозы	Источник и природа	Способ реализации	Используемые уязвимости	Объекты воздействия	Опасность угрозы	Возможность реализации	Актуальность
Информационные	Источник: внутренний и внешний. Природа: субъективные	Распространение нежелательной, недостоверной, противоречащей деятельности подразделения информации в электронном виде, а также нежелательный контент (фишинг), направленный на кражу персональной и конфиденциальной финансовой информации		Репутация и имидж структуры, конфиденциальная информация	Средняя	Средняя	актуальная
Программные	Источник: внутренний и внешний. Природа: субъективные	Вредоносные программы, специализированные программы (шпионское ПО) или не декларированные функциональные возможности (закладок) в программах	Не обновленный или нелицензионный антивирус, наличие закладок в программах, уязвимости в операционных системах, программах	Информация (данные) структуры в электронном виде, прикладные и системные программы, средства обработки, хранения и передачи информации, ЛВС, веб-ресурсы подразделения, файловое хранилище и базы данных информационных систем	Средняя	Средняя	актуальная
Сетевые	Источник: внутренний и внешний. Природа: субъективные	Сетевые атаки и воздействия, использующие каналы передачи информации и специальные программные средства, которые направлены на получение несанкционированного доступа для кражи, уничтожения или изменения информации, совершения противоправных действий, нарушение нормального функционирования	Уязвимости в сети, сетевых протоколах, программах и средствах	Информация (данные) структуры в электронном виде, прикладные и системные программы, средства обработки, хранения и передачи информации, ЛВС, веб-ресурсы подразделений, файловое хранилище, базы данных и информационные системы	Средняя	Средняя	актуальная

Наименование угрозы	Источник и природа	Способ реализации	Используемые уязвимости	Объекты воздействия	Опасность угрозы	Возможность реализации	Актуальность
Отказы в обслуживании технических и программных средств	Источник: внутренний и внешний. Природа: объективные и субъективные	Выход из строя или нарушение функционирования из-за морального износа или совершения ошибок со стороны обслуживающего персонала или воздействия на него нарушителя	Уязвимости в технических и программных средствах, уязвимости в процессах эксплуатации	Прикладные и системные программы, средства обработки, хранения и передачи информации, средства защиты информации	Средняя	Средняя	актуальная
Физические	Источник: внутренний и внешний. Природа: субъективные	Реализуются посредством физического доступа, физического взаимодействия (воздействия) нарушителя на объект защиты, которые направлены на уничтожение или разрушение, вывод из строя или нанесение вреда, совершение противоправных операций, хищение (кражу)	Уязвимости в средствах защиты от физического доступа	Информация в электронном виде и документированная информация, носители информации, каналы связи, технические средства обработки, хранения и передачи информации, и входящие в них программное обеспечение, помещения, шкафы и сейфы, иные материальные активы	Средняя	Средняя	актуальная

Наименование угрозы	Источник и природа	Способ реализации	Используемые уязвимости	Объекты воздействия	Опасность угрозы	Возможность реализации	Актуальность
Угрозы с использованием технических каналов утечки информации	Источник: внутренний и внешний. Природа: субъективные	Использование технических каналов утечек: электромагнитные сигналы, в том числе побочные электромагнитные излучения и наводки технических средств и каналов связи, акустические и виброакустические сигналы, электрические сигналы и радиоизлучения, оптические (телевизионные, фотографические и визуальные) сигналы в видимом, инфракрасном и ультрафиолетовом диапазонах волн	Наличие технических каналов утечек информации	Информация в электронном виде, технические средства обработки и хранения информации и каналы связи	Средняя	Низкая	актуальная
Техногенные	Источник: внутренний и внешний. Природа: объективные и субъективные	Пожары, взрывы, обрушения сооружений, затопления и иные бедствия, в том числе возникшие в результате стихийных природных явлений		Все объекты защиты	Средняя	Низкая	актуальная

Наименование угрозы	Источник и природа	Способ реализации	Используемые уязвимости	Объекты воздействия	Опасность угрозы	Возможность реализации	Актуальность
Организационно-правовые (юридические)	Источник: внутренний и внешний. Природа: субъективные	Нарушения требований законодательства и нормативной базы, регламента и требований по эксплуатации, выполнение неразрешенных действий персоналом, нарушение юридических прав, нелегальное использование программ и информационных материалов, невыполнение контрактных обязательств и т.д.	Уязвимости в правовых документах	Материальные и нематериальные активы, (имидж) сотрудники подразделения	Средняя	Низкая	не актуальная

Таблица №4. Анализ рисков и угроз информационной безопасности Университета

Объекты защиты	Актуальные угрозы	Последствия	Риски
Средства обработки и хранения информации (сервера и система хранения данных) информационных систем Университета	Заражение вредоносной программой	Нарушение нормального функционирования или полный выход из строя объекта защиты, которые будут определяться, исходя из опасности вируса и масштаба распространения вредоносной программы	Средний
	Отказ в обслуживании	Нарушение нормального функционирования, или выполнения отдельных технологических задач, или полный выход из строя объекта защиты	Средний
	Сетевые атаки, направленные на нарушение нормального функционирования (DoS, DDoS атаки)	Нарушение нормального функционирования или полный выход из строя объекта защиты	Средний
	Сетевые атаки, направленные на получение несанкционированного доступа	Нарушение нормального функционирования, доступ (нарушение конфиденциальности или целостности, модификация) к информации или (контроль управления, внесение изменений в настройку) к средствам	Средний
	Несанкционированный физический доступ	Нарушение нормального функционирования, доступ (нарушение конфиденциальности или целостности) к информации или (контроль управления, внесение изменений в настройку) к средствам	Средний
	Техногенные угрозы	Выход из строя средства, потеря информации	Ниже среднего
Программное обеспечение (операционные системы, СУБД, приложения и прикладное программное обеспечение)	Заражение вредоносной программой	Нарушение нормального функционирования, которое будет определяться, исходя из опасности вируса	Средний
	Отказ в обслуживании	Нарушение нормального функционирования, или выполнения отдельных технологических задач, или полный выход из строя информационной системы	Средний
	Сетевые атаки, направленные на получение несанкционированного доступа	Нарушение нормального функционирования, или полный выход из строя программы, или получение контроля и управления над программой	Высокий
	Несанкционированный	Нарушение нормального функционирования,	Средний

Объекты защиты	Актуальные угрозы	Последствия	Риски
	физический доступ	изменение настроек, модификация	
Сетевое оборудование и каналы связи для организации корпоративной сети ЛВС и подключения к внешней сети	Отказ в обслуживании	Нарушение нормального функционирования или выполнения отдельных технологических задач, или выход из строя средства, потеря связи	Средний
	Сетевые атаки, направленные на нарушение нормального функционирования (DoS, DDoS атаки)	Нарушение нормального функционирования или выход из строя средства, потеря связи	Средний
	Сетевые атаки, направленные на получение несанкционированного доступа	Нарушение нормального функционирования или получение контроля или управления над средством	Средний
	Несанкционированный физический доступ	Нарушение нормального функционирования или получение контроля или управления над средством, потеря связи	Средний
	Техногенные угрозы	Выход из строя средства, потеря связи	Ниже среднего
Средства защиты информации СУИБ	Отказ в обслуживании	Нарушение нормального функционирования или выполнения отдельных задач защиты или выход из строя средства	Средний
	Сетевые атаки, направленные на нарушение нормального функционирования (DoS, DDoS атаки)	Нарушение нормального функционирования и уровня защиты	Средний
	Сетевые атаки, направленные на получение несанкционированного доступа	Нарушение нормального функционирования и уровня защиты, получение контроля и управления над средством, изменение настроек	Средний
	Несанкционированный физический доступ	Нарушение нормального функционирования и уровня защиты	Средний
	Заражение вредоносной программой	Нарушение нормального функционирования, которое будет определяться, исходя из опасности вируса	Выше среднего
	Техногенные угрозы	Выход из строя средства, нарушение уровня	Ниже среднего

Объекты защиты	Актуальные угрозы	Последствия	Риски
		защиты	
Защищаемые помещения (серверное помещение, переговорная)	Несанкционированный физический доступ	Получение доступа к средствам и информации в помещении	Средний
	Техногенные угрозы	Потеря находящихся в помещении средств и информации (имущественные потери, нарушение функционирования)	Ниже среднего
Конфиденциальная информация	Несанкционированный физический доступ	Получение доступа (нарушение конфиденциальности или целостности) к информации	Средний
	Утечка информации по каналам связи (электронная почта, мессенджеры, сотовые телефоны и т.д.)	Утечка (нарушение конфиденциальности) информации	Выше среднего

10. Модель нарушителя информационной безопасности

10.1. Модель нарушителя формируется для систематизации данных о возможностях и типах субъектов, целях несанкционированных воздействий и выработки адекватных соответствующих методов противодействия. При разработке модели нарушителя должны учитываться:

- категории нарушителя;
- характеристики нарушителя для оценки степени опасности и важности и анализа его технической мощности.
- ограничительные меры и методы противодействия.

10.2. Нарушитель информационной безопасности – это лицо, которое предприняло попытку выполнения запрещенных операций (действий), направленных на нарушение информационной безопасности по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

10.3. Нарушителями по отношению к объектам защиты Университета могут быть сотрудники (подрядчики), имеющие непосредственный допуск к объектам защиты, и сотрудники (подрядчики), не имеющие такого допуска и получившие его не санкционированно к объектам защиты, так и лица, не являющиеся сотрудниками Университета.

10.4. Основные группы и классы нарушителей:

10.4.1. При рассмотрении нарушителей необходимо разделить их на группы по отношению к объектам защиты и соответственно возможностям воздействия на его компоненты. Групп нарушителей две:

1) внешние нарушители– физические лица, не обладающие правами доступа внутрь контролируемой зоны и соответственно не имеющие возможности прямого воздействия на объект защиты и его компоненты;

2) внутренние нарушители – физические лица, обладающие правами доступа внутрь контролируемой зоны и соответственно имеющие доступ к объекту защиты и его компонентам.

10.4.2. Вне зависимости от групп, нарушитель может относиться к одному из четырех классов по возможным действиям:

- первый (низкий) уровень (класс 1) возможностей нарушителя характеризуется запуском задач из фиксированного набора с заранее предусмотренными функциями по обработке информации;
- второй (класс 2), включает возможности пользователей первого уровня и дополнительно имеет возможности создания и запуска собственных программ с новыми функциями по обработке информации. Таким образом, возможна ситуация, когда внешний нарушитель реализует внутренние угрозы;
- третий (класс 3), имеет возможность управления функционированием объектом защиты, то есть воздействовать на базовое программное обеспечение, его состав и конфигурацию;
- четвертый (класс 4), отличается полным объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств объектов защиты, вплоть до включения в состав объекта защиты

технических и программных средств с новыми функциями по обработке данных.

10.4.3. Различение нарушителей по квалификации, как специалиста в области информационных технологий:

- неопытный пользователь (класс А): нарушитель этого класса предоставляет опасность как источник невнимательных или неверных действий на объект защиты, которые редко, но могут привести к сбою или даже отказу работы системы;

- уверенный пользователь (класс Б): данный класс нарушителя может быть источником нарушений работы объекта защиты, но попытки установить свои программы, воспользоваться внешними ресурсами, в том числе Интернет, будут пресечены системой разграничения доступа и средствами защиты информации;

- высококвалифицированный пользователь (класс В): все попытки нарушителя данного класса обойти установленные правила разграничения доступа и средства защиты информации должны фиксироваться системой аудита безопасности, блокироваться системой защиты.

10.5. Модели нарушителей информационной безопасности составляются и поддерживаются в отношении каждого важного и критичного объекта защиты Университета и включаются в модель угроз объекта защиты.

10.6. Модель нарушителей информационной безопасности для Университета включает следующих нарушителей с соответствующими категориями, характеристиками и ограничительными мерами в отношении них:

10.6.1. Внутренние нарушители:

1) Сотрудники Университета, являющиеся зарегистрированными (авторизованными) пользователями сетей и информационных систем Университета. По возможным действиям относятся к 1 классу, а по опытности – к классам А и Б.

Характеристики данного нарушителя: наличие возможности по реализации угроз, которые сводятся, в основном, к попыткам расширения своих полномочий и преодолению средств защиты информации с использованием только штатных программных и технических средств взаимодействия с объектом защиты, наличие возможности осуществления утечки защищаемой информации.

Ограничительные меры в отношении данных нарушителей: разграничение прав и управление доступом к объектам защиты, учет действий сотрудников в информационных системах, мониторинг возможных каналов утечек информации, контроль за соблюдением требований по неразглашению конфиденциальной информации.

2) Сотрудники Университета, не являющиеся пользователями информационных систем и сетей (охрана, технический персонал, обслуживающий здание и помещения и др.). По возможным действиям могут относиться к 1 классу и по опытности – к классу А.

Возможности по реализации угроз данного вида внутреннего нарушителя сводятся к получению несанкционированного физического доступа к объекту защиты и в основном выступают как источник невнимательных или неверных действий на объект защиты, которые могут привести к сбою или даже отказу работы системы.

Ограничительные меры в отношении данных нарушителей: выполнение требований по размещению объектов защиты, использование в отношении объекта комплекса режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированного физического доступа и действий, подбор и расстановка кадров, предоставление и управление допуском в помещения, в которых расположены объекты защиты.

3) Персонал, обслуживающий технические средства Университета. По возможным действиям относятся к 3 классу и по опытности – к классу В.

Характеристики данного нарушителя: наличие санкционированного доступа к техническим и программным средствам объекта защиты, но, не являясь их зарегистрированным пользователем. Возможности данного вида нарушителя существенным образом зависят от действующих ограничительных факторов по допуску физических лиц в помещения, в которых расположен объект защиты, и контролю за порядком проведения работ.

Ограничительные меры в отношении данных нарушителей: контроль порядка (регламента) проведения работ, наличие представителя Университета при проведении этих работ, предоставление доступа только к требуемым средствам объекта защиты, удаление или блокировка всех учётных данных подрядчика после исполнения им своей работы.

4) Администраторы, обслуживающие сети, информационные системы и средства защиты информации Университета. По возможным действиям относятся к 4 классу и по опытности – классам Б и В.

Характеристики данного нарушителя: наличие санкционированного доступа к объекту защиты и являются членами группы привилегированных пользователей. Особенность нарушителя данного вида состоит в том, что они входят в число доверенного персонала объекта защиты и им предоставляются широкие возможности для реализации угрозы по воздействию на внутреннее состояние компонентов объекта защиты.

Ограничительные меры в отношении данных нарушителей: учет и контроль действий данных сотрудников при обращении к объекту защиты.

5) Специалисты, являющиеся разработчиками информационных систем Университета. По возможным действиям относятся к 1 классу, а по опытности – к классам А и Б.

Характеристики данного нарушителя: наличие возможности по реализации угроз, которые сводятся к ошибкам разработчиков при разработке прикладной программы информационной системы или установке не декларированных функциональных возможностей (закладок) для совершения в дальнейшем противоправных действий, связанных с нарушением нормального функционирования прикладной программы или утечки информации.

Ограничительные меры в отношении данных нарушителей: учет и контроль действий данных сотрудников при разработке, осуществление анализа разработанных программ отдельными сотрудниками Университета с применением анализаторов исходного кода, тестирование функциональных возможностей, входных и выходных данных программы сторонними сотрудниками Университета.

10.6.2. Внешние нарушители:

1) Уволенные сотрудники Университета. По возможным действиям и опытности относятся к определённому классу в зависимости от ранее занимаемой им должности при работе в организации (бывший пользователь или не являвшийся пользователем сетей и информационных систем, или технический обслуживающий персонал, или администратор).

Характеристики данного нарушителя: возможности по реализации угроз данного вида внешнего нарушителя сводятся к раскрытию или использованию защищаемой информации Университета, в том числе технологической и технической по получению несанкционированного доступа и обходу средств защиты информации, с целью получения личной выгоды, нанесения ущерба бывшей организации, совершения противоправных действий.

Ограничительные меры в отношении данных нарушителей: выполнение обязательств по неразглашению конфиденциальной информации как уволенный сотрудник, исключение возможности использования их реквизитов доступа после увольнения.

2) Посетители, являющиеся представителями сторонних организаций, с которыми взаимодействует Университет при выполнении своей деятельности.

Характеристики данного нарушителя: возможности по реализации угроз данного вида внешнего нарушителя сводятся к получению несанкционированного физического доступа к объекту защиты.

Ограничительные меры в отношении данных нарушителей: выполнение требований по размещению объектов защиты, ограничение доступа посетителей в неразрешенные для них помещения (зоны) с применением комплекса режимных и организационно-технических мер.

3) Посетители, являющиеся представителями сторонних организаций, выполняющих какие-либо работы (поставщики услуг) в Университете. По возможным действиям могут относится ко 2-4 классу и по опытности – классам Б и В.

Характеристики данного нарушителя: наличие санкционированного доступа к объекту защиты, но не являясь их зарегистрированным пользователем – разработчики аппаратных и программных средств объекта защиты, осуществляющие их установку, пуско-наладочные работы, сопровождение в период эксплуатации и т.д. Особенность данного вида нарушителя в том, что он может осуществлять различные действия в зависимости от алгоритма функционирования, заложенного в специальных деструктивных средствах. Активизация специальных деструктивных средств может произойти в любой момент работы объекта защиты на протяжении всего его жизненного цикла.

Ограничительные меры в отношении данных нарушителей: контроль порядка(регламента) проведения работ, присутствие представителя Университета при проведении этих работ, предоставление доступа только к требуемым средствам объекта защиты.

4) Нарушители, получившие несанкционированный доступ к объекту защиты извне через внешнюю сеть, обойдя систему защиты. По квалификации данный нарушитель относится к классу В, а по возможным действиям может относится к 2 и 3 классу.

Характеристики данного нарушителя: совершение целенаправленных действий путем применения специальных программно-технических средств или уязвимостей в системе.

Ограничительные меры в отношении данных нарушителей: применение комплекса аппаратно-программных средств защиты, направленных на предотвращение и пресечение несанкционированных действий данных нарушителей.

11. Меры информационной безопасности

11.1. Для построения СУИБ в Университете должны реализовываться все меры обеспечения информационной безопасности, которые подразделяются на:

- правовые меры;
- морально-этические меры;
- организационные меры;
- технологические меры;
- инженерно-технические меры;
- программно-аппаратные меры;
- криптографические меры;
- меры безопасности в отношениях с внешними пользователями.

11.2. **Правовые меры**

11.2.1. Правовые меры реализуются путем проведения соответствующих мероприятий, связанных с формированием комплекса нормативных и организационно-распорядительных документов (правила, регламенты, порядки, положения, требования, инструкции, методики, руководства, обязанности, перечни, планы, мероприятия, формуляры и т.п.), регламентирующих вопросы обеспечения информационной безопасности в Университете в целом и на отдельных объектах защиты в частности.

11.2.2. Нормативная база Университета в области обеспечения информационной безопасности должна формироваться и вестись ОВИТиС.

11.2.3. Нормативная база Университета в области обеспечения информационной безопасности должна включать нормативно-правовые акты, включая международные и государственные стандарты Республики Узбекистан, а также внутренние документы Университета.

11.2.4. Ко внутренним документам Университета по обеспечению информационной безопасности относятся документы:

1) Определяющие перечень критичных и важных ресурсов защиты, их категорию и класс защищенности, включая перечень конфиденциальной информации.

К указанным документам относятся перечень конфиденциальной информации Университета, реестр информационных ресурсов Университета, перечень и классификатор объектов защиты Университета.

2) Организационно-распорядительного порядка, направленные на реализацию мер по обеспечению информационной безопасности, распределение обязанностей и ответственности среди сотрудников, а также обеспечения контроля за их действиями.

К указанным документам относятся планы мероприятий, приказы Университета о закреплении ответственности за подразделениями и отдельными сотрудниками Университета, положения управления, отделов, служб, центров, кафедры других структурных подразделений Университета, а также должностные инструкции сотрудников Университета;

3) Устанавливающие порядок и регламентирующие процессы, и процедуры обеспечения информационной безопасности.

К данным документам относятся положения, правила и порядок проведения процедурных вопросов, инструкции по эксплуатации и эксплуатационная документация;

4) Журналы, отчеты, заявки, протоколы и другие документы, используемые для регистрации и подтверждения выполненных процедур и работ по обеспечению информационной безопасности.

Отдельные внутренние документы Университета по обеспечению информационной безопасности приведены в приложениях к настоящей Политике.

11.2.5. Разработку внутренних нормативных документов по обеспечению информационной безопасности в Университете осуществляет ОВИТиС.

11.2.6. Внутренние нормативные документы по информационной безопасности и изложенные в них требования должны доводиться ответственными должностными лицами до сведения сотрудников Университета, на которых распространяется действие этих документов, и содержащиеся в них требования должны ими строго соблюдаться.

11.3. **Морально-этические (психологические) меры защиты информации**

11.3.1. Морально-этические (психологические) меры защиты информации обеспечиваются в соответствии с Морально-этическим кодексом Университета.

Морально-этические (психологические) меры защиты информации направлены на:

- создание здорового морального климата среди сотрудников;
- снижение вероятности возникновения негативных действий и нарушений информационной безопасности, связанных с человеческим фактором;

- исключение личностных психологических факторов при нарушении режима защиты информации;
- соблюдение сотрудниками Университета правил этического поведения.

11.3.2. Морально-этические меры защиты являются профилактическими, к которым относятся:
- проведение разъяснительных работ среди сотрудников Университета;
- психологический мониторинг;
- принуждение и применение дисциплинарных мер в отношении нарушителей;
- побуждение и поощрение сотрудников.

11.3.3. Разъяснительные работы проводятся ОВИТиС среди сотрудников Университета в виде специальных занятий или индивидуальных бесед.

11.3.4. Данная разъяснительная работа направлена на:
- повышение уровня знаний сотрудников касательно влияния угроз на деятельность Университета и о возможных последствиях, а также о мерах ответственности, которые могут быть применены в отношении нарушителей;
- выработку сознания у сотрудников в необходимости выполнения элементарных процедур и требований настоящей Политики информационной безопасности;
- повышение степени сознательности и ответственности сотрудников Университета в вопросах обеспечения информационной безопасности;
- выработку требуемых норм поведения и нравственности, которые способствуют соблюдению правил и требований обеспечения информационной безопасности;
- создание сплоченности сотрудников при решении задач обеспечения информационной безопасности.

11.3.5. Разъяснительные работы проводятся не реже одного раза в год отдельно для следующих групп сотрудников Университета:
- сотрудников, входящих в руководящий состав Университета;
- сотрудников подразделений Университета;
- сотрудников Университета, обеспечивающих обслуживание информационных систем и ресурсов, технического и технологического оборудования информационно-коммуникационной инфраструктуры Университета.

11.3.6. В отношении новых сотрудников Университета должен проводиться вводный инструктаж по вопросам обеспечения информационной безопасности.

11.3.7. Психологический мониторинг применяется как к отдельной личности, так и к организации в целом, что позволяет быстро выявить какие-либо волнения среди сотрудников, определять ответственных и добросовестных сотрудников в отношении соблюдения правил и норм, так и безответственных и халатных сотрудников, которых следует взять на контроль и принять в отношении них соответствующие меры.

11.3.8. Меры принуждения должны быть направлены для создания условий, при которых сотрудники Университета будут вынуждены соблюдать правила и требования по обеспечению информационной безопасности, а именно меры наказания на случай их нарушения.

11.3.9. В отношении нарушителей руководством Университета могут применяться меры дисциплинарного взыскания в соответствии с законодательством и руководящими документами Национальной гвардии Республики Узбекистан.

11.3.10 Меры побуждения должны быть направлены для создания условий, которые мотивируют сотрудников Университета к должному поведению. К данным мерам относятся поощрительные меры.

11.3.11. В отношении отличившихся сотрудников, надлежаще выполняющих трудовые обязательства, должны приниматься поощрительные меры в виде объявления благодарности, предоставления почетных грамот, денежной премии или ценного подарка, а за особые услуги представлены к государственным наградам в порядке, установленном законодательством.

11.3.12. В целях предупреждения правонарушений, устранения причин и условий, способствующих их совершению, со стороны всех сотрудников Университета должны соблюдаться требования законодательства, в т.ч. Уставы Вооруженных Сил Республики Узбекистан и руководящие документы Национальной гвардии Республики Узбекистан, а также приказы и распоряжения командования Университета.

.

11.4. **Организационные меры**

11.4.1. Организационные меры в Университете направлены на:

- распределение обязанностей и ответственности между подразделениями и сотрудниками;
- определение и классификацию объектов защиты, анализ и оценку рисков информационной безопасности;
- защиту и неразглашение конфиденциальной информации;
- создание, функционирование и развитие системы и средств защиты информации;
- реагирование на инциденты информационной безопасности;
- повышение уровня квалификации и осведомленности сотрудников в области обеспечения информационной безопасности;
- оценку уровня защищенности;
- обеспечение физической защиты.

11.4.2. В части распределения обязанностей и ответственности между подразделениями и сотрудниками Университета принимаются следующие организационные меры:

а) назначение ответственного из числа руководства Университета, который будет отвечать за все вопросы, связанные с обеспечением информационной безопасности в Университете, и ответственного сотрудника по информационной безопасности в Университете среди сотрудников

ОВИТиС, а также администраторов информационной безопасности в каждом из подразделений Университета среди руководителей подразделений (начальников или их заместителей);

б) назначение администратора корпоративной сети и администраторов ЛВС, системных администраторов информационных систем;

в) определение списка лиц, получающие как физический, так и логический доступ к объектам информатизации Университета, в том числе к конфиденциальной информации, серверному помещению, ЛВС, сетевому оборудованию, информационным системам и ресурсам, средствам защиты информации;

г) определение лиц, ответственных за функционирование и эксплуатацию конкретных средств обработки, хранения, передачи и защиты информации;

д) закрепление соответствующими организационно-распорядительными документами учетных съемных носителей и накопителей данных за сотрудниками Университета;

е) осуществление со стороны ОВИТиС контроля за выполнением ответственными лицами, закрепленных за ними обязанностей в части обеспечения информационной безопасности.

Распределение обязанностей между сотрудниками, ответственными за обеспечение информационной безопасности должно осуществляться в соответствии с разделом 14 настоящей Политики.

Задачи по обеспечению информационной безопасности в Университете возлагаются на ОВИТиС, что определено в их функциональных обязанностях, приведенном в приложении №5 к настоящей Политике.

Обязанности и ответственность ответственного сотрудника по информационной безопасности в Университете, а также администраторов информационной безопасности определены в приложениях №6 и №7 к настоящей Политике соответственно, а администратора корпоративной сети и администраторов ЛВС – в приложениях №3 и №4 к настоящей Политике соответственно.

11.4.3. В части определения и классификации объектов защиты, анализа и оценки рисков информационной безопасности принимаются следующие организационные меры:

а) проведение инвентаризации для определения объектов защиты и информационных активов;

б) формирование списка объектов защиты и реестра информационных ресурсов Университета, определение класса защищенности для каждого объекта или ресурса;

в) определение модели угроз для каждого объекта защиты и проведение анализа и оценки рисков информационной безопасности в соответствии с разделом 9 настоящей Политики.

Инвентаризация, классификация, маркировка и формирование реестра информационных активов (ресурсов) должны производиться в соответствии с Порядком управления информационными активами, приведенным в приложении №15 к настоящей Политике.

Инвентаризация осуществляется в рамках внутреннего аудита, который организуется и проводится ответственным сотрудником по информационной безопасности совместно с подразделением ОВИТиС не реже одного раза в год. По итогам инвентаризации при необходимости вносятся изменения и дополнения в список объектов защиты и в реестр информационных ресурсов Университета. Дополнительно по результатам инвентаризации определяется перечень помещений, состав комплекса технических и программных средств, входящих в объект информатизации.

Классификация объектов защиты осуществляется в соответствии с требованиями нормативных документов.

11.4.4. В части защиты и неразглашения конфиденциальной информации принимаются следующие организационные меры:

а) строгое регламентирование документов по грифам согласно руководящих документов НГ РУз;

б) определение и утверждение списка лиц, допущенных к каждой категории информации, входящей в перечень конфиденциальной информации согласно полученного в установленном порядке допуске;

в) определение требований по сохранности конфиденциальной информации и ответственности за ее разглашение и утрату;

г) при приеме сотрудников на работу и ознакомление их под роспись с перечнем конфиденциальной информации и мерами ответственности за её разглашение и утрату.

Для сотрудников, допущенных к конфиденциальной информации, их обязательства по сохранности конфиденциальной информации и ответственность определяются руководящими документами НГ РУз.

11.4.5. В части создания, функционирования и развития системы и средств защиты информации принимаются следующие организационные меры:

а) закупка средств защиты информации в рамках реализации мероприятий по обеспечению информационной безопасности Университета;

б) определение технических требований к закупаемым средствам защиты информации;

в) проведение организационных мероприятий по подготовке к внедрению и обеспечению эксплуатации системы и средств защиты информации, к которым относятся выделение помещения, разработка инструкций по эксплуатации, закрепление ответственного сотрудника и прохождение им обучения по эксплуатации;

г) проведение опытно-эксплуатационных и приемно-сдаточных испытаний при внедрении средств защиты информации;

д) осуществление управления (администрирования) системой защиты, включающего в себя контроль конфигурации и параметров настройки, восстановление работоспособности, контроль установки обновлений программного обеспечения, корректировку эксплуатационной документации, контроль за событиями безопасности, документирование процедур и результатов контроля;

е) подготовка и внесение предложений по совершенствованию системы защиты информации в случае выявления недостатков в функционировании и обеспечении защищенности.

11.4.6. В части выявления, ликвидации последствий и проведения расследований по инцидентам информационной безопасности принимаются организационные меры, которые определены в разделе 12, а также в приложении №19 к настоящей Политике.

11.4.7. В части повышения уровня квалификации и осведомленности сотрудников в области обеспечения информационной безопасности принимаются следующие организационные меры:

а) прохождение переподготовки и повышения квалификации сотрудниками Университета, ответственными за обеспечение информационной безопасности (ответственный сотрудник по информационной безопасности Университета, администраторы информационной безопасности объектов всех подразделений Университета), на регулярной основе, не реже одного раза в год;

б) организация и проведение обучения сотрудников Университета с целью повышения их осведомленности и выполнение ими требований и положений настоящей Политики;

в) проведение аттестации сотрудников Университета по итогам обучения для проверки уровня их осведомленности;

г) ознакомление каждого сотрудника Университета с необходимыми разделами настоящей Политики информационной безопасности под роспись в журнале, форма которой приведена в приложении №21.

Для повышения квалификации сотрудников, ответственных за обеспечение информационной безопасности, а также обучения сотрудников Университета по вопросам защиты информации ОВИТиС совместно с ответственными подразделениями ежегодно составляется и утверждается график курсов повышения квалификации и обучения основам информационной безопасности.

Инструктажи и обучение сотрудников Университета по вопросам обеспечения информационной безопасности и разделам настоящей Политики информационной безопасности проводятся ответственным сотрудником по информационной безопасности Университета и/или администраторами информационной безопасности на объектах подразделений Университета.

Журналы ознакомления сотрудников Университета с Политикой информационной безопасности и прочими политиками в сфере ИКТ Университета ведутся на постоянной основе на всех объектах структуры и их сохранность обеспечивается ответственными сотрудниками по информационной безопасности на каждом из объектов.

11.4.8. В части оценки уровня защищенности принимаются следующие организационные меры:

а) проведение внутреннего и внешнего аудита для оценки уровня защищенности объектов защиты и актуализации настоящей Политики;

б) организация проведения аттестации объектов информатизации Университета аккредитованными организациями согласно постановлению

Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»;

в) проведение экспертизы официального веб-сайта Университета на соответствие требованиям информационной безопасности;

г) проведение оценки эффективности принятых организационных, технических и иных мер защиты, а также устранение выявленных недостатков по итогам аудитов, экспертиз и аттестаций.

Регулярность проведения внутреннего аудита должна составлять не менее 1 раза в год, а внешнего аудита – не менее 1 раза в три года.

Внутренний аудит проводится ответственным сотрудником по информационной безопасности совместно с подразделением ОВИТиС Университета. При необходимости в нём могут участвовать сотрудники подразделений УС,ИКТиЗИ НГ РУ. Для проведения внешнего аудита информационной безопасности привлекаются сторонние организации, компетентные проводить такой аудит.

11.4.9. В части обеспечения физической защиты принимаются следующие организационные меры:

а) организация охраны и пропускного режима на входе в территорию и здания объектов подразделений Университета. Охрана на входе обеспечивается суточными нарядами сотрудников Университета;

б) размещение объектов информатизации на максимально возможном расстоянии относительно границы контролируемой зоны;

в) размещение основных технических средств обработки, хранения, передачи и защиты информации (сервера информационных систем, сетевое оборудование, средства защиты информации) - в защищаемом серверном помещении;

г) установка оборудования в серверном помещении, а также коммутаторов внутри зданий в запираемых коммутационных шкафах;

д) хранение документированной конфиденциальной информации и съемных носителей конфиденциальной информации в сейфах, шкафах или иных защищенных хранилищах, учет носителей конфиденциальной информации.

11.5. **Технологические меры**

11.5.1. Технологические меры обеспечения информационной безопасности Университета направлены на:

- обеспечение пожарной безопасности и климатических условий для нормального функционирования средств обработки и хранения информации;
- резервирование технических средств обработки, хранения, передачи и защиты информации;
- резервирование каналов связи;
- резервирование информации и информационных ресурсов;
- обеспечение гарантированного электропитания;
- обеспечение информационной безопасности при выводе из эксплуатации объектов защиты.

11.5.2. В основных помещениях зданий Университета, а также в серверном и коммутационных помещениях объектов подразделений Университета используется система пожарной сигнализации.

11.5.3. В серверном и во всех коммутационных помещениях, а также на площадках установки телекоммуникационного оборудования (коммутационные шкафы, коммутаторы, источники бесперебойного питания и оборудование беспроводной связи) на объектах подразделений Университета следует применять средства обеспечения требуемых для оборудования климатических условий для долговременной эксплуатации.

Для обеспечения нормального функционирования серверного помещения, оно должно полностью отвечать требованиям O‘zDSt 2875:2014 «Требования к дата-центрам. Обеспечение инфраструктуры и информационной безопасности».

11.5.4. Резервированию подлежат следующие технические средства Университета:

- серверы информационных систем Университета, размещенные в серверном помещении Университета;
- маршрутизаторы, используемые для подключения серверов ко внешней и внутренней корпоративной сети;
- коммутаторы ядра корпоративной сети;
- телекоммуникационное оборудование;
- каналы связи;
- межсетевые экраны и средства IDPS, используемые на границе подключения оборудования серверного помещения ко внешней и внутренней корпоративной сети.

11.5.5. Резервированию подлежат каналы связи, используемые для подключения в серверном помещении Университета к внешней и корпоративной сети.

11.5.6. Требования по резервированию средств обработки, хранения, передачи и защиты информации, а также каналов связи определены в Плане обеспечения непрерывной работы и восстановления работоспособности в чрезвычайных (аварийных) ситуациях, приведенном в приложении №19 к настоящей Политике.

11.5.7. Резервному копированию подлежит база данных и журналы (логи) информационных систем Университета, а также конфигурируемые параметры (настройки) сетевого оборудования и средств защиты информации. Для размещения и хранения резервных копий Университетом должна быть приобретена и оборудована соответствующая система хранения данных. Пропускная способность сети передачи данных должна позволять успешно завершить процесс резервного копирования данных с удалённых объектов в нерабочее время (с 20:00 до 08:00 следующего дня) на ежедневной основе. Резервное копирование и восстановление данных в Университете осуществляется в соответствии с Положением по обновлению системного и прикладного программного обеспечения, а также резервному копированию и

восстановлению данных, приведенным в приложении №8 к настоящей Политике.

11.5.8. Для обеспечения бесперебойного электропитания Университета предусмотрены следующие меры:

- использование дизель-генератора для бесперебойного питания серверного и сетевого оборудования и средств защиты информации серверного помещения в здании УМСЦ Университета(по адресу: Ташкентская область, Зангиотинский район, посёлок Чорсу);
- подача резервного электропитания в здания;
- использование источников бесперебойного питания UPS для серверов, сетевого оборудования, средств защиты информации в серверном и коммутационных помещениях на объектах всех подразделений Университета.

11.5.9. В целях обеспечения информационной безопасности при выводе из эксплуатации объектов защиты или после принятия решения об окончании обработки информации должны выполняться меры по уничтожению (безопасное стирание) данных и любой остаточной информации с носителей информации и (или) меры по физическому уничтожению носителей информации по согласованию с руководством Университета.

11.5.10. Уничтожение (безопасное стирание) данных и остаточной информации с носителей информации и (или) физическое уничтожение носителей информации при выводе их из эксплуатации осуществляется в соответствии с Инструкцией по обеспечению безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных, приведенной в приложении №11 к настоящей Политике.

11.5.11. Документированная конфиденциальная информация подлежит уничтожению с применением специального уничтожителя (шредер).

11.6. **Инженерно-технические меры**

11.6.1 Инженерно-технические меры направлены на предотвращение физического доступа или создания препятствий для проникновения посторонних физических лиц к объектам защиты и включают следующие меры:

1) применение на входе в Университет и его подразделения системы контроля доступа сотрудников (СКУД) – в настоящее время СКУД установлен на входе: КПП 1, здания УМСЦ, помещения ЗАС ОВИТиС, кафедры ТСП, помещения дежурной службы, помещения ОРС и ОПиБП;

2) использование системы распознавания лиц СКУД FaceID сотрудников при доступе на территорию Университета;

3) установка на входе в серверное помещение Университета железной двери;

4) использование на входе в серверное помещение Университета кодового замка;

5) установка железных решеток на окнах серверного помещения Университета (при их наличии);

6) применение системы видеонаблюдения на входе в серверное помещение Университета, а также на территории и внутри зданий для видеоконтроля за периметром зданий, входом в здания, коридорами зданий объектов Университета и его подразделений;

7) установка охранной сигнализации в защищаемых помещениях, в том числе в серверном помещении;

8) использование запираемых железных несгораемых шкафов для хранения документированной конфиденциальной информации и съемных носителей конфиденциальной информации;

9) опечатывание корпусов рабочих станций, серверов, сетевого оборудования и средств защиты информации для блокировки физического доступа к ним;

10) установка серверов, сетевого оборудования и средств защиты информации в специальных стойках, которые запираются механическим замком;

11) прокладка сетевых кабелей в защищенных местах внутри зданий и вне их в соответствии с требованиями раздела 13 настоящей Политики.

11.7. **Программно-аппаратные меры**

11.7.1. Программно-аппаратные меры обеспечения информационной безопасности Университета направлены на:

- организацию технической защиты информации;

11.7.2. Для обеспечения технической защиты информации применяются следующие средства технической защиты информации:

- межсетевые экраны;
- средства IDPS;
- средства антивирусной защиты информации;
- средства разграничения доступа;
- средства предотвращения утечек конфиденциальной информации;
- средства контроля и анализа защищенности, а также мониторинга и управления инцидентами информационной безопасности;
- средства мониторинга функционирования и др.

11.7.3. Применяемые в Университете аппаратные средства, программные продукты, информационно-коммуникационные технологии, телекоммуникационное оборудование и иные технические средства, в том числе средства защиты информации должны сертифицироваться в соответствии с требованиями постановления Президента Республики Узбекистан от 15 июня 2020 года ПП-4751 «О мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан».

11.7.4. Используемые методы и средства технической защиты информации в Университете приведены в Инструкции по организации технической защиты информации в приложении №16 к настоящей Политике.

11.7.5 Обеспечение безопасности сетевой инфраструктуры и применение межсетевых экранов осуществляется в соответствии с Положением по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование, приведенным в приложении №2 к настоящей Политике.

11.7.6. Для защиты от вредоносных программ принимаются технические меры в соответствии с Инструкцией по антивирусной защите, приведенной в приложении №10 к настоящей Политике.

11.7.7. Для разграничения доступа к информационным ресурсам и системам Университета разрабатывается матрица доступа в соответствии с Правилами по разработке матрицы доступа к информационным ресурсам, приведенными в приложении №12 к настоящей Политике.

В Университете применяются средства разграничения доступа посредством применения уникальных учётных записей пользователей корпоративного домена, предоставляемого каждому сотруднику Университета в целях обеспечения персонализированного использования всех ИКТ-сервисов структуры и для закрепления сферы его ответственности при информационном взаимодействии.

11.7.8. Аутентификация пользователей при доступе к объектам защиты осуществляется по паролям и иным идентификаторам, которые формируются и используются в соответствии с Инструкцией по парольной защите, приведенной в приложении №9 к настоящей Политике.

11.8. **Криптографические меры**

11.8.1Защита конфиденциальной информации в Университете организуется с применением СКЗИ.

11.8.2 Криптографическая защита информации в Университете используется для:

- организации защищенных соединений в корпоративной сети Университета;
- для защищенного обмена информацией с применением систем E-XAT, в которых обеспечивается шифрование и целостность передаваемой информации.

11.8.3. В Университете должны использоваться СКЗИ, прошедшие сертификацию в органе по сертификации СКЗИ в соответствии с постановлением Президента Республики Узбекистан от 3 апреля 2007 года №ПП-614.

11.8.4. Используемые методы и средства криптографической защиты информации в Университете приведены в Инструкции по организации криптографической защиты информации в приложении №17 к настоящей Политике.

11.9 **Меры безопасности в отношениях с внешними пользователями**

11.9.1. Меры безопасности в отношениях с внешними пользователями направлены на:

- исключение несанкционированного физического доступа внешних пользователей к объектам защиты Университета и его средствам;
- исключение несанкционированного сетевого доступа внешних пользователей сторонних организаций при доступе к информационным системам и ресурсам Университета, а также при взаимодействии со сторонними информационными системами.

11.9.2. К мерам безопасности в отношениях с внешними пользователями для исключения их несанкционированного физического доступа относятся:

1) ведение журнала прихода и ухода посетителей со сторонних организаций на объектах Университета;

2) сопровождение посетителей внутри здания сотрудниками Университета;

3) прием посетителей и проведение встреч с представителями сторонних организаций в отдельных комнатах приема;

4) определение требований по нераспространению конфиденциальной информации третьим лицам в договорах со сторонними организациями, осуществляющими разработку, обслуживание или поставку программного обеспечения и оборудования для Университета.

11.9.3. При обеспечении доступа сотрудников сторонних организаций, являющихся разработчиками, поставщиками оборудования и т.д. к объектам защиты Университета на основании заключенных с ними договоров, в данных договорах или в отдельных заключаемых с ними соглашениях должен быть определен перечень конфиденциальной информации, а также условия и требования по её нераспространению третьим лицам. Также со стороны сторонней организации должны быть определены конкретные лица, которые будут получать доступ к объектам защиты и такой доступ должен предоставляться только этим лицам.

11.9.4. Лица от сторонних организаций, допущенных к объектам защиты Университета, должны находиться и выполнять работы в присутствии сотрудника Университета.

11.9.5. К мерам безопасности в отношениях с внешними пользователями для обеспечения защищенного обмена информации при их подключении к информационным системам и ресурсам (официальный веб-сайт Университета), также при взаимодействии со сторонними информационными системами относятся организация защищенных соединений в соответствии с требованиями Положения о корпоративной сети и организации защищенных сетевых соединений, приведенного в приложении №1 к настоящей Политике.

11.9.6. Для исключения несанкционированного сетевого доступа внешних пользователей при доступе к информационным системам и ресурсам Университета должны обеспечиваться меры межсетевого экранирования в соответствии с Положением по обеспечению информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование, приведенным в приложении №2 к настоящей Политике, а также аутентификации пользователей при доступе к информационным системам Университета в соответствии с Инструкцией по парольной защите, приведенной в приложении №9 к настоящей Политике.

12. Реагирование на инциденты информационной безопасности

12.1. Одним из важных процессов в комплексной СУИБ Университета является процесс управления инцидентами информационной безопасности.

12.2. Основными целями процесса управления инцидентами информационной безопасности являются:

- минимизация потерь Университета, вызванных инцидентами информационной безопасности, за счет обеспечения оперативного выявления инцидентов информационной безопасности, устранения угроз, ликвидации последствий инцидентов и восстановления данных и функционирования объектов защиты;
- снижение риска возникновения повторных инцидентов за счет принятия мер, исключающих или минимизирующих возможность их повторного возникновения.

12.3. Основными процессами управления инцидентами информационной безопасности являются:

- быстрое обнаружение инцидентов информационной безопасности;
- анализ данных о событиях информационной безопасности;
- регистрация инцидента информационной безопасности;
- реагирование на инциденты информационной безопасности и информирование о них руководства Университета и при необходимости заинтересованные сторонние организации (например, ГУП «Центр кибербезопасности»);
- установление источников и причин возникновения инцидентов, а также оценка их последствий;
- получение достоверной и полной информации о нарушениях информационной безопасности в Университете после обнаружения инцидента, оценка его последствий;
- минимизация нарушений порядка работы и повреждения данных информационных систем и иных объектов защиты Университета, восстановление в кратчайшие сроки данных и их работоспособности;
- анализ результатов устранения последствий инцидента информационной безопасности;
- проведение расследований по инцидентам информационной безопасности, обеспечение сохранности и целостности доказательств возникновения инцидента информационной безопасности, создание условий для накопления и хранения точной информации об имевших место инцидентах информационной безопасности;
- выработка рекомендаций и мер по недопущению повторного возникновения инцидентов информационной безопасности;
- обучение персонала Университета действиям по обнаружению, устранению последствий и предотвращению инцидентов информационной безопасности, отработка ими планов восстановлений на случай аварийных и чрезвычайных ситуаций.

12.4. В Университете должны быть определены лица, ответственные за выявление инцидентов и за реагирование на них, а также на всех объектах должны вестись Журналы учета инцидентов информационной безопасности, форма которых приведена в приложении к Инструкции ответственного сотрудника по информационной безопасности в Университете согласно приложению №6 к настоящей Политике.

12.5. В журнале учета инцидентов информационной безопасности должны фиксироваться все инциденты информационной безопасности, возникшие на объектах Университета.

В журнале учета инцидентов информационной безопасности и нештатных ситуаций должны указываться даты и время событий, вид событий, объекты защиты, с которым связано событие, и характер последствий.

В журнале должно фиксироваться достаточное количество информации об аварийных состояниях и действительных событиях информационной безопасности с тем, чтобы можно было осуществлять тщательный анализ предполагаемых и фактических инцидентов информационной безопасности.

12.6. Журнал учета инцидентов информационной безопасности в Университете ведется ответственным сотрудником по информационной безопасности.

12.7. Фиксации и учету подлежат следующие события информационной безопасности:

- нарушение конфиденциальности, целостности и доступности информации;
- нарушение технологического процесса;
- нештатные чрезвычайные ситуации (пожары, наводнения и иные стихийные бедствия или техногенные аварии);
- пропадание связи со внешними сетями и с корпоративной сетью передачи данных Университета;
- отказ основного сетевого, серверного оборудования, средств защиты информации по любым причинам, как технического, так и программного характера;
- нарушение работы программного обеспечения информационных систем и ресурсов;
- неавторизированный или несанкционированный доступ третьих лиц к информационным системам и ресурсам;
- нарушение любых правил обработки, хранения, передачи информации;
- отказ в обслуживании DoS (Denial of Service) и DDoS (Distributed Denial of Service);
- выявленные средствами защиты сетевые атаки и вторжения;
- сбои (перезагрузки) в работе ЛВС, корпоративной сети, серверов и установленного на них программного обеспечения, средств защиты информации;
- аномальная сетевая активность и аномальное поведение приложений;

- подключение новых сетевых узлов и появление новых служб;
- утеря и кража средств, носителей и самой информации;
- выявление уязвимостей;
- переустановка операционной системы или программ приложений на серверах информационных систем;
- изменение аппаратной конфигурации, настроек и параметров информационной безопасности;
- выявленные неправомерные действия по сбору информации;
- выявленные опасные вирусы и вредоносные программы;
- утечка, удаление, неправомерный доступ к защищаемой информации;
- иные нарушение правил, определенных настоящей Политикой информационной безопасности.

12.8. Для выявления событий информационной безопасности должен вестись постоянный мониторинг, который должен охватывать:
- журналы (лог-файлы) межсетевых экранов, маршрутизаторов, коммутаторов, серверов, рабочих станций, веб-приложений, операционных систем, СУБД и т.д.;
- визуальный контроль состояния работоспособности средств;
- выходные данные средств защиты информации, включая средства защиты от вредоносных программ, межсетевые экраны, средства обнаружения и предотвращения вторжений IDPS и т.д.;
- результаты проведения внутреннего или внешнего аудита информационной безопасности;
- информацию о событиях и инцидентах, о которых сообщили сотрудники и вспомогательный персонал.

12.9. Ответственными за выявление и реагирование на инциденты информационной безопасности являются:
- ЛВС, сетевое оборудование объектов Университета – администраторы ЛВС объектов Университета и сотрудники администрирования серверов и сетевого оборудования ОВИТиС;
- рабочие станции объектов Университета – сотрудники ОВИТиС и УМСЦ;
- серверное оборудование и программное обеспечение серверного помещения (сервер контроллер корпоративного домена, сервера корпоративной электронной почты, официального веб-сайта, веб-приложений и баз данных информационных систем) – системные администраторы (сотрудники УМСЦ);
- корпоративная сеть – администратор корпоративной сети (сотрудники ОВИТиС и УМСЦ);
- средства защиты информации (антивирусы, межсетевые экраны, IDPS и др.) – администраторы, обслуживающие данные средства (сотрудники ОВИТиС и УМСЦ).

12.10. Иные сотрудники Университета в случае выявления инцидента информационной безопасности обязаны сообщить об этом начальнику ОВИТиС Университета вне зависимости от места работы. Данные

сотрудники не должны принимать несогласованные с указанными специалистами действия по ликвидации последствий инцидентов, с тем, чтобы не увеличить их последствия.

12.11. Сотрудники, ответственные за выявление и реагирование на инциденты информационной безопасности, обязаны доложить об инцидентах своему непосредственному начальнику и администратору информационной безопасности объекта Университета.

12.12. Администраторы информационной безопасности объектов Университета обязаны сообщать о выявленных инцидентах ответственному сотруднику по информационной безопасности Университета с предоставлением ему полной и объективной информации (время возникновения, характер угрозы, причины и источники угроз, подверженные объекты защиты, масштабы последствий, принятые первоочередные меры).

12.13. В свою очередь ответственный сотрудник по информационной безопасности Университета обязан докладывать об инцидентах заместителю начальника университета по развитию информационных технологий (Digital Chief Oficer) с фиксацией времени и прочей информации об инциденте в Журнале учета инцидентов информационной безопасности Университета.

12.14. В случае возникновения событий информационной безопасности, приведших к существенным нежелательным и негативным последствиям информационной безопасности, о них должны сообщаться руководителям объектов и руководству Университета.

12.15. По каждому инциденту информационной безопасности определяются причины возникновения инцидента, источник угрозы, оцениваются масштабы последствий, принимаются меры по устранению угрозы, ликвидации последствий инцидента, а также при необходимости дополнительные меры по повышению защищенности для предотвращения повторных появлений подобных инцидентов.

12.16. Устранение последствий проводится специалистом, ответственным за обслуживание объекта защиты, при необходимости по решению начальника ОВИТиС к устранению последствий привлекаются дополнительные специалисты и ресурсы.

К устранению последствий могут быть привлечены сторонние эксперты или специалисты обслуживающей организации. В случае, когда внешние эксперты или специалисты обслуживающей организации участвуют в ликвидации последствий инцидентов, с ними должно быть заключено соглашение о неразглашении конфиденциальной информации.

12.17. При реагировании на выявленные инциденты информационной безопасности ответственный сотрудник по информационной безопасности Университета должен взаимодействовать с ГУП «Центр кибербезопасности» в соответствии с Регламентом взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по

реагированию, расследованию и предотвращению инцидентов информационной безопасности.

12.18. Для проведения расследований инцидентов создается группа из специалистов Университета.

12.19. При расследовании выявляются истинные причины инцидента, нарушители и вырабатываются рекомендации для предотвращения повторного возникновения данного инцидента. На основе данных рекомендаций ОВИТиС принимаются и реализуются меры для предотвращения повторения инцидента.

12.20. К расследованию инцидентов с тяжкими последствиями с целью привлечения к ответственности нарушителей должны привлекаться правоохранительные органы.

12.21. Решение о проведении специального расследования инцидента, сообщение о них внешним заинтересованным сторонам и привлечение правоохранительных органов принимается руководством Университета, исходя из тяжести и последствий произошедшего инцидента.

12.22. При реагировании на инциденты информационной безопасности сотрудники должны руководствоваться Регламентом обработки инцидентов, аварийных и чрезвычайных ситуаций, а также взаимодействия со сторонними организациями, приведенным в приложении №19 к настоящей Политике.

13. Обеспечение безопасности каналов связи

13.1. Кабели электропитания и сетевые кабели, используемые для передачи данных, необходимо защищать от вскрытия в целях исключения перехвата информации и их повреждения. Для уменьшения такого риска реализуются следующие защитные меры:

а) кабели электропитания и связи должны проводиться (по возможности) под землей, в канализациях и коллекторах, а внутри зданий в коробах или защищены надлежащим образом от несанкционированного физического доступа;

б) для защиты сетевых кабелей от их несанкционированного вскрытия и перехвата данных, а также от повреждения, используются экранированные кабели, которые прокладываются так, чтобы они не проходили через общедоступные места. При отсутствии технической возможности прокладки кабелей в обход общедоступных мест, такие кабели должны укладываться в металлические короба, конструкция которых исключает возможность их несанкционированного вскрытия;

в) незадействованные разъемы сетевых кабелей, предназначенные для подключения рабочих станций, должны опечатываться или заклеиваться специальной маркой для исключения возможного несанкционированного подключения нештатных технических средств обработки информации;

г) кроссовое и коммутационное оборудование с подключенными к нему сетевыми кабелями должно размещаться в закрываемом серверном помещении и в закрываемых коммутационных шкафах.

д) незадействованные сетевые порты телекоммуникационного оборудования и серверного оборудования должны быть отключены программными средствами управления телекоммуникационным оборудованием и средствами управления серверным оборудованием.

13.2. Сетевые кабели, по мере возможности, должны пролегать отдельно от электрических, чтобы исключить негативное влияние друг на друга (магнитные помехи), а также быть защищены от неавторизованных подключений или повреждений, например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход общедоступных участков.

13.3. В целях обеспечения конфиденциальности информации при передаче её по сетям телекоммуникаций реализуются следующие защитные меры:

а) использование защищенных https-соединений с применением протоколов https, SSL/TLS при обеспечении подключения сотрудников к информационным системам Университета и пользователей к информационным системам и официальному веб-сайту Университета;

б) использование защищенных систем передачи информации, таких как система защищенной электронной почты E-XAT для обмена сообщениями (корреспонденцией) между объектами Университета, а также со сторонними организациями;

в) применение защищенных VPN-соединений при соединении с внешними пользователями для автоматизации процесса.

13.4. При передаче информации ограниченного доступа по каналам связи, выходящим за пределы контролируемой зоны, должно обеспечиваться шифрование информации сертифицированными в Республике Узбекистан средствами криптографической защиты информации.

14. Распределение ответственности

14.1. Для создания и поддержания режима информационной безопасности, необходимо четкое и документальное закрепление ответственности за информационную безопасность отдельных ресурсов и за выполнение определенных процедур защиты информации.

14.2. Ответственность за распределение ресурсов и внедрение процедур информационной безопасности возлагается на руководителей Университета.

14.3. Основными обязанностями руководства Университета при обеспечении информационной безопасности являются:

- определение целей обеспечения информационной безопасности;
- формулировка, пересмотр и утверждение Политики информационной безопасности;
- контроль эффективности внедрения настоящей Политики;
- обеспечение четкого и единого руководства и ощутимой административной поддержки всем инициативам, направленным на повышение безопасности;
- выделения необходимых средств на обеспечение информационной безопасности;
- назначение ответственных за информационную безопасность в пределах Университета и за определение их обязанностей;
- инициирование планов и программ поддержания осведомленности персонала по информационной безопасности.

14.4. Непосредственная организация и эффективное функционирование СУИБ в Университете возлагается на начальника ОВИТиС и ответственного сотрудника по информационной безопасности Университета.

Задачи и функции ОВИТиС в части обеспечения информационной безопасности определены в приложении №5 к настоящей Политике, а обязанности ответственного сотрудника по информационной безопасности – в приложении №6 к настоящей Политике.

14.5. Настоящая Политика устанавливает следующее распределение ответственности за обеспечение безопасности в Университете:

- за всю деятельность по обеспечению информационной безопасности в Университете несут ответственность заместитель начальника университета по развитию информационных технологий (Digital Chief Oficer), отвечающий за все вопросы, связанные с обеспечением информационной безопасности в

Университете, начальник ОВИТиС и ответственный сотрудник по информационной безопасности Университета;

- за обеспечение информационной безопасности на объектах Университета несут ответственность их администраторы информационной безопасности;

- за хранение доверенной сотруднику информации (в любом её виде) и обеспечение должного уровня её защиты данный сотрудник несет персональную ответственность;

- за действия, совершаемые в информационных системах Университета, несут ответственность сотрудники Университета в рамках, закрепленных за ними ролей и обязанностей;

- за информационную безопасность (в т.ч. физическую) рабочей станции несет ответственность сотрудник Университета, которому данная рабочая станция предоставлена для исполнения служебных обязанностей;

- за информационную безопасность ЛВС Университета несет ответственность администратор ЛВС объекта, являющийся сотрудником отдела ОВИТиС;

- за целостность и функционирование корпоративной сети Университета и циркулирующей в ней информации, её доступность и конфиденциальность, несёт ответственность администратор корпоративной сети, являющийся сотрудником ОВИТиС;

- за целостность и функционирование официального веб сайта Университета, его доступность и конфиденциальность, несёт ответственность администратор официального веб-сайта Университета – начальник УМСЦ;

- за информационную безопасность информационных систем несут ответственность начальник ОВИТиС, сотрудник по информационной безопасности (за каждой информационной системой закрепляется конкретный системный администратор);

- за пожарную и техническую безопасность, сохранность оборудования внутри каждого помещения несет ответственность сотрудник, назначенный соответствующим распоряжением руководителя структурного подразделения Университета, в котором находится данное помещение и размещено данное оборудование.

14.6. Указанная в пункте 14.5 ответственность определяется в должностных инструкциях сотрудников и других внутренних нормативных документах Университета.

Сотрудник, за которым закреплена ответственность по обеспечению информационной безопасности ресурса, может частично или полностью передавать полномочия по обеспечению её защиты, однако, ответственность за данный ресурс продолжает оставаться за ним.

14.7. На время отсутствия ответственного (отпуск, болезнь, командировка и пр.) его обязанности выполняет лицо, назначенное в установленном порядке. Данное лицо приобретает соответствующие права

и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

15. Порядок пересмотра и актуализации Политики

15.1. В настоящую Политику могут вноситься изменения и дополнения в следующих случаях:

- вступления отдельных пунктов Политики информационной безопасности в противоречие с новыми или измененными законодательными и иными нормативно-правовыми актами, нормативными документами по информационной безопасности;
- необходимости пересмотра требований обеспечения информационной безопасности;
- изменения конфигурации и состава информационной инфраструктуры Университета, появления новых объектов защиты информации;
- изменения состава средств защиты информации;
- изменения структуры (реорганизации) Университета.

15.2. В случае вступления отдельных пунктов настоящей Политики в противоречие с новыми законодательными актами Республики Узбекистан в области защиты информации, а также иными нормативными актами Университета, данные пункты утрачивают юридическую силу до момента внесения дополнений и изменений в Политику информационной безопасности.

15.3. Изменения и дополнения в настоящую Политику вносятся по инициативе ОВИТиС и утверждаются решением руководства правления Университета.

15.4. Полный пересмотр Политики информационной безопасности должен осуществляться в случае реконструкции информационно-коммуникационной инфраструктуры Университета и связанных с ней информационно-технологических процессов, реорганизации Университета, влекущих изменения структуры его СУИБ.

15.5. Новая редакция Политики подлежит повторному согласованию с Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан, Службой государственной безопасности Республики Узбекистан и ГУП «Центр кибербезопасности».

15.6. Актуализация и оценка эффективности Политики информационной безопасности осуществляется путем проведения внутреннего и внешнего аудита информационной безопасности. Аудит проводится на предмет:

- оценки выполнения требований и положений утвержденной Политики информационной безопасности;
- соответствия информационно-коммуникационной инфраструктуры Университета установленным требованиям информационной безопасности;
- оценки эффективности принятых мер, методов и средств защиты информации;
- необходимости внесения изменений, дополнений или пересмотра настоящей Политики информационной безопасности.

15.7. Регулярность проведения внутреннего аудита должна составлять не реже 1 раза в год, а внешний аудит – не реже 1 раза в 3 года.

15.8. Внутренний аудит организуется Заместителем начальника университета по развитию информационных технологий (Digital Chief Oficer) и проводится совместно с подразделениями Университета. Для проведения внешнего аудита информационной безопасности привлекаются сторонние организации, компетентные проводить такой аудит.

15.9. По результатам аудита и/или в процессе реализации в Политику информационной безопасности Университета могут вноситься изменения и дополнения с целью приведения её в соответствие с реальными условиями и требованиям защиты информации. Решение о внесении в Политику информационной безопасности Университета изменений и дополнений принимается начальником ОВИТиС и выносится на согласование руководству Университета.

15.10. Сотрудники Университета должны ознакомиться с Политикой информационной безопасности после её утверждения или пересмотра под роспись в Журнале ознакомления с Политикой информационной безопасности, форма которой приведена в приложении №21 к настоящей Политике.