« УТВЕРЖДАЮ »

Ташкентский Международный Университет Кимё

_____А.Б.Аллакулиев

«____» _____ 20____ г

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАШКЕНТСКОГО МЕЖДУНАРОДНОГО УНИВЕРСИТЕТА КИМЁ

I.Общие положения

1. Настоящая Концепция информационной безопасности Ташкентского международного университета Кимё (далее — ТМУК) определяет стратегию обеспечения информационной безопасности в процессе формирования, обработки, передачи и хранения информации в информационной системе ТМУК
2. Концепция информационной безопасности ТМУК (далее — Концепция) является основополагающим документом, устанавливающим цели, задачи, принципы и основные меры по защите информации..
3. Действие Концепции распространяется на всех сотрудников и пользователей, имеющих доступ к информационной системе ТМУК.
4. В настоящей Концепции используются следующие термины и определения:

- **Авторизация** — предоставление пользователю прав доступа;
- **Аутентификация** — подтверждение подлинности пользователя;
- **Внешние каналы передачи данных** — каналы передачи данных не подконтрольные работникам ТМУК;
- **Секреты** — сведения особой важности;
- **Демилитаризованная зона** — особая зона в информационной системе, создаваемая для передачи данных с одного уровня доступа на другой, имеющая специфичные в зависимости от характера выполняемых в зоне операций, требования к информационной безопасности;(VLAN)
- **документированная информация** — информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать.
- **зашита информации** — меры по предотвращению угроз информационной безопасности и устранению их последствий;
- **информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от источников и формы их представления;

- **информационная система ТМУК** — совокупность технических и программных средств ТМУК, с учетом имеющихся требований по их обособленному и совместному функционированию;
- **конфиденциальная информация** — документированная информация, доступ к которой ограничивается;
- **несанкционированный доступ к информации** — доступ к информации, осуществленный с нарушением установленных правил разграничения доступа;
- **обслуживающий персонал информационной системы** — совокупность сотрудников, ответственных за сопровождение информационной системы;
- **пользователь информационной системы** — лицо вне зависимости от места работы, осуществляющее подключение, приём или передачу информации в информационной системе;
- **угроза информационной безопасности** — потенциальная возможность преднамеренного или неумышленного воздействия в информационной системе, которая может прямо или косвенно нанести ущерб пользователям или владельцам информационной системы;
- **физическое разделение сети** — разделение сети передачи данных на несколько самостоятельных сетей, не связанных аппаратными средствами;

II. Цель и задачи Концепции

5. Основной целью Концепции является формирование общей стратегии в области обеспечения информационной безопасности информационной системы ТМУК.
6. Основными задачами Концепции являются:

- формирование основных принципов построения системы обеспечения информационной безопасности;
- формирование основных требований к функционированию системы обеспечения информационной безопасности;
- формирование организационно-методической базы для реализации системы обеспечения информационной безопасности;
- определение приоритетных направлений, позволяющих развитию системы обеспечения информационной безопасности.

III. Основные принципы Концепции

7. Концепция основывается на следующих принципах:

- защита любой информации, противоправное обращение с которой может причинить ущерб ТМУК;
- соответствие системы обеспечения информационной безопасности требованиям законодательства Республики Узбекистан;
- поэтапное развитие системы обеспечения информационной безопасности, с учетом действующей организационной структуры ТМУК и приоритетности внедрения мер по обеспечению информационной безопасности;
- обеспечение надлежащей осведомленности и обучения работников и пользователей информационной системы ТМУК в области информационной безопасности;
- создание эффективной системы финансирования мероприятий по обеспечению информационной безопасности.

IV. Правовые основы формирования Концепции

8. Нормативные документы, разработанные в соответствии с Концепцией, должны соответствовать требованиям законодательства, а также документам по информационной безопасности ТМУК.
9. В целом по организации систем информационной безопасности ТМУК применяются стандарты в области информационных технологий и информационной безопасности, принятые ТМУК.
10. ТМУК обеспечивает ознакомление соответствующих работников с актами законодательства, а также стандартами в области информационных технологий и информационной безопасности.

V. Объекты защиты и оценка рисков

11. Информационная система ТМУК является распределенной системой, объединяющей в единую информационно-телекоммуникационную сеть, в которой совместно используется информация, подлежащей защите.
12. Обеспечение функционирования и сопровождение информационной системы ТМУК осуществляется Центром цифровых технологий (далее — ЦЦТ).
13. Информация, циркулирующая в информационной системе ТМУК, разделяется на следующие уровни:
    - Информация с ограниченным доступом, находящаяся в информационной системе ТМУК;

- Общедоступная информация, находящаяся в информационной системе ТМУК.

14. К конфиденциальной информации относятся:
    - персональные данные сотрудников;
    - служебная информация;
    - информация, ограниченная приказами.
15. К внутренней общедоступной информации относится информация, формируемая и используемая сотрудниками в информационной системе ТМУК в рамках выполнения своих должностных обязанностей, за исключением информации, относящейся к внутренней информации с ограниченным доступом.
16. Основные угрозы безопасности информации в информационной системе ТМУК проявляются в следующих видах:
    - несанкционированное разглашение, утечка, хищение информации;
    - несанкционированное блокирование или уничтожение информации, нарушение технологических процессов, дезорганизация работы информационной системы, разрушение информационных, программных средств информационной системы;
    - искажение, подмена, фальсификация информации;
    - сбои системы.
17. По характеру возникновения угрозы информационной безопасности разделяются на следующие группы:

    а) искусственные угрозы, которые в свою очередь делятся на:
    - **непреднамеренные угрозы**: ошибочные, случайные, необдуманные, без злого умысла и корыстных целей нарушения установленных регламентов сбора, обработки и передачи информации, а также требований информационной безопасности и другие действия лиц, приводящие к непроизводительным затратам времени и ресурсов, разглашению информации с ограниченным доступом, потере ценной информации или нарушению работоспособности отдельных рабочих станций, подсистем или информационной системы в целом;
    - **преднамеренные угрозы**: нарушения в корыстных целях, по принуждению третьими лицами, со злым умыслом и другие нарушения установленных регламентов сбора, обработки и передачи информации, а также требований информационной безопасности и другие действия лиц, приводящие к непроизводительным затратам времени и ресурсов, разглашению информации с ограниченным доступом, потере ценной информации или нарушению

работоспособности отдельных рабочих станций, подсистем или информационной системы в целом;

б) естественные угрозы:

- отказы, аварии и сбои программно-технических средств, возникшие в результате стихийных бедствий, природных катаклизмов и др.

18. Эксплуатация аппаратно-программных комплексов, содержащих внутреннюю информацию ограниченного доступа, разрешается только после принятия необходимых мер по защите информации. Процедуры и инженерно-технические меры защиты должны быть направлены:
    - на предотвращение угрозы, или локализацию воздействия угрозы информационной безопасности;
    - на восстановление работоспособности информационной системы в случае необходимости.
19. Для каждой информации, а также для каждого вида внутренней информации с ограниченным доступом, должны быть определены сроки доступности.
20. Для перевода информации из одного уровня доступа на другой уровень должны быть созданы соответствующие процедуры и демилитаризованные зоны.

VI. Пути противодействия угрозам информационной безопасности

21. Основные меры, направленные на обеспечение требуемого уровня информационной безопасности, подразделяются на:
    - физические меры защиты;
    - организационные меры защиты;
    - инженерно-технические меры зашиты,
22. Физические меры зашиты основываются на применении разного рода механических, электронных, электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам информационной системы и защищаемой информации, а также технических средств визуального наблюдения и охранной сигнализации.
23. Физическая защита зданий и помещений, в которых размещены основные компоненты информационной системы ТМУК, осуществляется силами охраны.
24. Физические меры защиты помещений должны обеспечить:
    - предотвращение проникновения к защищаемому объекту посторонних лиц;

- круглосуточное наблюдение защищаемого объекта, где размещены основные компоненты информационной системы;
- идентификацию каждого лица, посещающего зачищаемые объекты, ведение журнала, содержащего-информацию о посещении лицами;
- блокирование всевозможных путей проникновения и доступа к защищаемому объекту в чрезвычайных случаях.

25. Организационные (административные) меры защиты регламентируют процесс функционирования системы обработки данных, использование информации, деятельность обслуживающего персонала, а также взаимодействие пользователей с информационной системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз информационной безопасности или снизить размер потерь в случае их реализации.
26. Главной целью организационных мер, предпринимаемых на высшем управленческом уровне, является принятие решений и разработка документов в области информационной безопасности, предусматривающих в том числе:
    - выделение необходимых человеческих и денежных ресурсов;
    - проведение регулярных проверок над состоянием информационной безопасности;
    - реализацияя мероприятий, направленных на обеспечения информационной безопасности ТМУК.
27. ТМУК разрабатывает инструкции, положения и другие нормативные документы. определяющие порядок:
    - предоставления доступа к внутренней информации с ограниченным доступом;
    - проведения обслуживания, модификации аппаратно-программных средств, ремонта аппаратных средств соответствующего категории доступа;
    - ведения баз данных в информационной системе;
    - пользования информационной системой пользователями;
    - предоставления доступа к внутренней общедоступной информации;
    - сопровождения информационной системы обслуживающим персоналом;
    - осуществления мер в чрезвычайных случаях;
    - предоставление доступа работников ТМУК и других лиц к использованию информационной системы, должно осуществляться в соответствии с утвержденным порядком;

28. Уровень полномочий каждого пользователя информационной системы определяется индивидуально, с соблюдением следующих требований:
    - предоставление доступа пользователям к информации, только входящей в его служебные обязанности;
    - в процессе предоставления доступа пользователям к информационной системе соблюдается принцип «явно неразрешенные полномочия и права считаются запрещенными»;
    - администрирование и сопровождение информационной системы должно производиться с разграничением обязанностей, прав и полномочий между администраторами операционной системы и системы управления базами данных, администраторами приложения, администраторами локальной вычислительной сети и администраторами информационной безопасности;
    - все сотрудники, допущенные к работе в информационной системе, обслуживающий персонал несут персональную ответственность за нарушения установленного порядка автоматизированной обработки данных, правил хранения, использования и передачу находящихся в их распоряжении информации и аппаратно-программных средств;
    - Каждый сотрудник при приеме на работу должен подписывать Соглашение-обязательство о соблюдении установленных правил работы с защищаемой информацией в информационной системе ТМУК и ответственности за их нарушение;
29. Все операции по ведению баз данных, любые изменения в базе данных, изменения состава и полномочий пользователей (в том числе обслуживающего персонала) базы данных в информационной системе ТМУК должны осуществляться в соответствии с утвержденным порядком.

30. Сохранность информации баз данных обеспечивается организацией ежедневного ведения электронного архива в соответствии с утвержденными технологическими инструкциями. При этом необходимо соблюдать нижеследующие требования:
    - архивирование базы данных производится в полном объеме с учетом программного комплекса и вспомогательных средств управления;
    - организация хранения электронных архивов на внешних энергетически независимых носителях информации;
    - организация плановых или внештатных проверок электронных архивов, для определения пригодности их восстановлению;

- организация резервной системы обработки данных, полностью или частично дублирующей активные системы обработки данных, отдаленной от основного центра обработки данных.

31. Все процессы обслуживания и осуществления модификации аппаратно-программных средств, а также ввод в эксплуатацию новых аппаратно-программных средств, подсистем и все изменения в конфигурации технических и программных средств, подсистем в информационной системе ТМУК должны осуществляться только на основе утвержденного порядка.
32. Все аппаратные и программные средства ТМУК должны быть в установленном порядке категорированы по уровню доступа (для информации, хранящейся, обрабатывающейся с использованием соответствующих аппаратно-программных средств должен быть определен требуемый уровень доступа, который присваивается соответствующим аппаратным и программным средствам).
33. Конфигурация аппаратно-программных средств должна соответствовать возложенным на пользователей обязанностям и требованиям по информационной безопасности исходя из ее характера и уровня доступа.
34. Не входящая в обязанности работника информация (программные средства, игры, кинофильмы, клипы и др.) не должна храниться на аппаратно-программных средствах, подключенных к информационной системе ТМУК, должна быть незамедлительно удалена при обнаружении.
35. Инженерно-технические меры защиты должны основываться на использовании различных электронных устройств и специальных программ, входящих в состав информационной системы ТМУК, выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты информации.
36. При условии соблюдения действующих требований и процедур информационной безопасности инженерно-технические меры защиты информации должны обеспечивать:
    - доступность, целостность и конфиденциальность информации, циркулирующей в информационной системе ТМУК;
    - контроль доступа к информационной системе и регистрацию всех событий; рациональное использование ресурсов информационной системы;
    - целостность и работоспособность системы обеспечения информационной безопасности;
    - выявление и предотвращение угроз информационной безопасности;

- резервирование и восстановление данных.

37. Инженерно-технические меры защиты должны включать в себя:
    - средства идентификации, аутентификации пользователей (в том числе администраторов) и элементов информационной системы (рабочих станций, терминалов, элементов баз данных и др.), средства разграничения и контроля доступа к информационной системе;
    - средства, обеспечивающие бесперебойное функционирование информационной системы;
    - средства архивирования и хранения информации;
    - антивирусные средства защиты информации;
    - другие современные программные и аппаратные средства защиты информации.
38. Аутентификация пользователей должна осуществляться на основе использования паролей в зависимости от характера информации и категории доступа.
39. Средства разграничения доступа к информационной системе должны осуществлять авторизацию пользователя после его распознавания информационной системой.
40. Авторизация пользователя должна осуществляться с использованием следующих механизмов реализации разграничения доступа:
    - избирательного управления доступом, основанных на использовании атрибутных схем, списков разрешений и другие;
    - полномочного управления доступом, основанных на использовании меток конфиденциальности информации и уровней доступа пользователей;
    - обеспечения замкнутой среды доверенного программного обеспечения;
41. Технические средства разграничения доступа должны быть составной частью единой системы контроля доступа
42. Информационная система ТМУК должна включать в себя средства, обеспечивающие бесперебойное функционирование (дублирующие элементы системы, источники бесперебойного питания, электрогенераторы и другие).
43. Основными требованиями к средствам, обеспечивающим бесперебойное функционирование информационной системы, являются:
    - автоматическое реагирование на выход из строя, отключение (включение) основного узла информационной системы, электрического питания и обеспечение бесперебойного

функционирования информационной системы в течение установленного времени;

44. Средства архивирования и хранения информации должны обеспечивать надежное функционирование информационной системы путём восстановления информации в случае необходимости.
45. Основными требованиями к организации ведения электронного архива в информационной системе ТМУК являются:
    - назначения ответственного сотрудника по введению работ по электронному архивированию и резервному копированию;
    - надежное хранение архивированных данных;
46. Основными требованиями к организации антивирусной защиты информации в информационной системе ТМУК являются:
    - исользование лицензированного антивирусного программного обеспечения;
    - организация постоянной антивирусной проверки;
    - обеспечение актуальности состояния антивирусных баз (списка сигнатур) антивирусного программного обеспечения как на административной части (сервера и другие), так и на пользовательской части (персональные компьютеры пользователей) информационной системы, путём автоматического или ручного обновления;
    - организация регулярной проверки работоспособности антивирусной системы;
    - организация выявления источника распространения компьютерных вирусов в информационной системе;

VII. Реализации Концепции

47. Для реализации Концепции необходимо:
    а) в зависимости от характера и категории информации применять многослойную систему защиты информации:
        - первый слой защиты — физическое ограничение доступа к аппаратно-программным средствам информационной системы;
        - второй слой защиты — идентификация и аутентификация пользователя,
    б) довести до пользователей изменения в требованиях законодательства по информационной безопасности, которые имеют к ним непосредственное отношение;

48. На подразделение по информационной безопасности возлагаются следующие функции:

- контроль над доступом пользователей в информационную систему, включая установку, периодическую смену паролей;
- контроль хранения резервных копий баз данных информационной системы, создания и хранения базы данных систем информационной безопасности;

IX. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

49. Концепция подлежит регулярному пересмотру и обновлению.
50. Изменения утверждаются руководством ТМУК.

Проректор по стратегическому развитию и цифровизации _____ Восиқов У.А.

Руководитель/директор центра цифровых технологий _____ Ли И.Г.