НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«КАРАГАНДИНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ИМЕНИ АБЫЛКАСА САГИНОВА»

Кафедра ИТБ

СОЛОДОВНИКОВА И.В.

**КОНСПЕКТ ЛЕКЦИЙ**

по дисциплине

Дисциплина SSSIB 2301 Сертификация и стандартизация средств информационной безопасности

Модуль PO 08 Профессионально-ориентированный 1

Образовательная программа 6В06301 «Системы информационной

безопасности»

Обсуждены на заседании кафедры «Информационные технологии и безопасность»

Протокол № 20а от «14» 05 2024г.

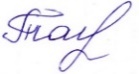


Зав. кафедрой \_\_\_\_\_\_\_\_\_\_ Коккоз М.М. «14» 05 2024г.

Одобрены Комитетом по обеспечению качества факультета инновационных

технологий

Протокол № 7 от «21» 05 2024г.



Председатель \_\_\_\_\_\_\_\_\_\_ Тау А.Ғ. «21» 05 2024г.

Караганда 2024

**Тема 1** Стандартизация, сертификация, аккредитация, лицензирование и разрешения в сфере обеспечения ИБ (3 часа)

План лекции

1. Стандартизация
2. Сертификация, аккредитация в РК
3. Лицензирование

В РК вопросы стандартизации регламентируются Законом Республики Казахстан от 5 октября 2018 года № 183-VІ ЗРК «О стандартизации».

*Стандартизация* – деятельность, направленная на обеспечение безопасности и качества объектов стандартизации и достижение оптимальной степени упорядочения требований к объектам стандартизации посредством установления положений для всеобщего, многократного использования в отношении реально существующих и потенциальных задач.

*Объектами стандартизации* являются продукция, процессы и услуги, подлежащие или подвергшиеся стандартизации.

*Субъектами национальной системы стандартизации* являются государственные органы, а также физические и юридические лица, осуществляющие деятельность в сфере стандартизации.

*Целями стандартизации* являются:

1. повышение конкурентоспособности отечественной продукции, процессов и услуг;
2. экономия природных и энергетических ресурсов;
3. обеспечение национальной безопасности и социально-экономического развития государства;
4. повышение безопасности и качества продукции, процессов и услуг;
5. устранение технических барьеров в торговле для создания условий интеграции в международную систему стандартизации;
6. предупреждение действий, вводящих в заблуждение потребителей относительно безопасности и качества продукции, процессов и услуг;
7. поддержка эффективного внедрения инноваций и развития высокотехнологичных производств, а также содействие трансферту технологий и наилучших лабораторных практик;
8. создание условий для улучшения безопасности и качества жизни населения.

Национальная система стандартизации – совокупность субъектов и их отношений в процессе осуществления деятельности в сфере стандартизации, а также документов по стандартизации и нормативных технических документов, являющихся объектами общедоступного государственного информационного ресурса**.**

Структуру национальной системы стандартизации составляют:

1) Правительство Республики Казахстан;

2) уполномоченный орган;

3) государственные органы в пределах своей компетенции;

4) национальный орган по стандартизации;

5) технические комитеты по стандартизации;

6) технические эксперты по стандартизации;

7) физические и юридические лица.

К документам по стандартизации (*документ по стандартизации – документ, устанавливающий нормы, правила, характеристики, принципы, касающиеся различных видов деятельности в сфере стандартизации или ее результатов*) относятся:

* международные стандарты, классификаторы технико-экономической информации международных организаций по стандартизации;
* стандарты, классификаторы технико-экономической информации, правила, нормы и рекомендации по стандартизации иностранных государств;
* региональные стандарты, классификаторы технико-экономической информации, правила и рекомендации по стандартизации региональных организаций по стандартизации;
* национальные стандарты и национальные классификаторы технико-экономической информации;
* рекомендации по стандартизации;
* стандарты организаций.

Национальные, межгосударственные стандарты и национальные классификаторы технико-экономической информации являются обязательными для применения, если имеются указания об этом в законодательстве Республики Казахстан (*пример – в постановлении Правительства РК № 832 «Об утверждении единых требований в области ИКТ и обеспечения ИБ» в пункте 29 приводится требование – «При организации, обеспечении и управлении ИБ в ГО, МИО или организации необходимо руководствоваться положениями стандарта Республики Казахстан СТ РК ISO/IEC 27002-2015 "Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации"»*).

При этом, ссылки на стандарты организаций не могут применяться в нормативных правовых актах.

Документы по стандартизации применяются на добровольной основе вне зависимости от страны и места происхождения объектов стандартизации, если иное не установлено законодательством Республики Казахстан в сфере стандартизации.

Применение физическими и юридическими лицами документов по стандартизации осуществляется с соблюдением авторских прав.

Международные организации по стандартизации в сфере ИТ и ИБ

К международным организациям, участвующим в международной стандартизации относятся:

1. Международная организация по стандартизации (ИСО, https://www.iso.org/ru/home.html) - организация по стандартизации, членство в которой открыто для соответствующего государственного органа по стандартизации, метрологии и сертификации каждой страны.
2. Международная электротехническая комиссия ([iec.ch](http://iec.ch/)) создана в 1906 году на международной конференции, в которой участвовали 13 стран, в наибольшей степени заинтересованных в такой организации.
3. Стандартизация, сертификация и метрология в рамках СНГ осуществляется в соответствии с «Соглашением о проведении согласованной политики в области стандартизации метрологии и сертификации», которое является межправительственным и действует с 1992 г. В соответствии с данным Соглашением были признаны: действующие ГОСТы в качестве межгосударственных стандартов. На межправительственном уровне был создан Межгосударственный совет по стандартизации, метрологии и сертификации (МГС, https://easc.by).
4. Национальный Институт Стандартов и Технологий (NIST, [www.nist.gov](http://www.nist.gov/)), США - основан в 1901 году и до 1988 года известен как Национальное бюро стандартов (National Bureau of Standards (NBS)). Институт является подразделением Управления по технологиям США, одного из агентств Департамента торговли США.
5. Американский национальный институт стандартов (ANSI, ansi.org) - объединение американских промышленных и деловых групп, разрабатывающие торговые и коммуникационные стандарты. Входит в организации ISO и IEC, представляя там интересы США. ANSI был создан 19 октября 1918 года..
6. DIN - Немецкий институт по стандартизации (Deutsches Institut fuer Normung e. V.) - создан в 1917 году. В 1975 году был признан немецким правительством как национальная организация по разработке стандартов. Сегодня DIN продвигает идею «Industry 4:0», объединяя различные организации в государственном и частном секторах, для принятия совместных решений относительно стандартов по «Industry 4:0».

В РК вопросы сертификации и аккредитации регламентируются Законом Республики Казахстан от 30 декабря 2020 года № 396-VI ЗРК «О техническом регулировании».

Закон устанавливает принципы технического регулирования, возникающие при установлении, исполнении требований к продукции, связанным с ней процессам, оказанию услуг, а также определяет правовые основы функционирования государственной системы технического регулирования.

Объектами технического регулирования являются:

* продукция, за исключением продукции используемой в целях защиты сведений, составляющих государственную тайну (государственные секреты) или относящихся к охраняемой в соответствии с законами РК информации ограниченного доступа;
* связанные с требованиями к продукции процессы проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;
* услуги в части добровольной сертификации, за исключением услуг в области ветеринарии, защиты и карантина растений, государственных, медицинских, образовательных, финансовых, банковских и других услуг, регулирование которых установлено иными законами РК, актами Президента РК и Правительства РК.

Оценка соответствия выпускаемой в обращение продукции требованиям технических регламентов и (или) документов по стандартизации осуществляется до выпуска ее в обращение, если иное не установлено техническим регламентом.

Испытание проводится в независимой и не заинтересованной в результатах оценки соответствия лаборатории, аккредитованной *(аккредитация — процедура официального подтверждения соответствия объекта установленным критериям и показателям (стандарту)* в соответствии с законодательством Республики Казахстан об аккредитации в области оценки соответствия. Испытательная лаборатория (центр) – юридическое лицо или структурное подразделение юридического лица, действующее от его имени, осуществляющее испытания (исследования);

В сфере информатизации и обеспечения ИБ подтверждению соответствия (сертификации) (*сертификация – процедура, посредством которой орган по подтверждению соответствия удостоверяет соответствие продукции и (или) связанного с ней процесса, а также услуги установленным требованиям*) и регистрации деклараций о соответствии подвергается продукция:

* электротехническая;
* радиотехническая;
* электронная;
* программные средства и базы данных (исходные коды ПО);
* кабельная продукция;
* система менеджмента информационной безопасности.

В РК вопросы лицензирования регламентируются Законом Республики Казахстан от 16 мая 2014 года № 202-V ЗРК «О разрешениях и уведомлениях».

Лицензирование — это процедура, которая предполагает выдачу государством разрешения компаниям или частным лицам на ведение определенного вида деятельности. Это обязательное условие для ведения предпринимательской деятельности в Казахстане. Лицензии РК — это свидетельства квалификации предпринимателя, который производит и продает товары и услуги.

Статья 28 Закона содержит все лицензируемые виды деятельности. Подробный реестр лицензий РК представлен в первом приложении к закону. В нем описаны подвиды по каждому пункту. Все, что не вошло в список, — это виды деятельности, не подлежащие лицензированию в РК.

Лицензируемые виды деятельности в сферах информатизации и связи, обеспечения ИБ:

* 1. обеспечение информационной безопасности:
* Лицензия на разработку средств криптографической защиты информации;
* Лицензия на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий;
  1. специальные технические средства, предназначенные для проведения оперативно-розыскных мероприятий;
* Лицензия на осуществление деятельности по разработке, производству, ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий:

1. Разработка, производство специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий;

2. Ремонт и реализация специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий;

3)предоставление услуг в области связи:

* Междугородная телефонная связь;
* Международная телефонная связь;
* Спутниковая подвижная связь;
* Сотовая связь.
  1. деятельность в сфере цифровых активов
* Лицензия на осуществление деятельности по цифровому майнингу:

1. I подвид – осуществление деятельности по цифровому майнингу цифровым майнером, имеющим на праве собственности или других законных основаниях центр обработки данных цифрового майнинга.
2. II подвид – осуществление деятельности по цифровому майнингу цифровым майнером, не имеющим на праве собственности или других законных основаниях центр обработки данных цифрового майнинга и осуществляющим цифровой майнинг с использованием принадлежащего ему на праве собственности аппаратно-программного комплекса для цифрового майнинга, размещенного в центре обработки данных цифрового майнинга.

Закон РК «Об информатизации» определяет следующие виды деятельности, требующие лицензии:

* «*Статья 7-2. Оперативный центр информационной безопасности.*

*….*

*пункт 2. Оперативный центр информационной безопасности осуществляет свою деятельность на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий*.»

* «*Статья 7-3. Служба реагирования на инциденты информационной безопасности*

*…..*

*пункт 2. Служба реагирования на инциденты информационной безопасности осуществляет свою деятельность на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий.*»

В РК активно развивается информационная система «Е-лицензирование» (https://elicense.kz/) посредством которой предприниматели могут подавать заявления на около 500 видов деятельности. Заявления принимают и обрабатывают соответствующие госорганы. По результатам проверок выдается электронная лицензия.

Рекомендуемая литература

1 Закон РК «О стандартизации» от 5 октября 2018 года № 183-VІ ЗРК

2 Закон РК «О техническом регулировании» от 30 декабря 2020 года № 396-VI ЗРК

3 Закон РК «О разрешениях и уведомлениях» от 16 мая 2014 года № 202-V ЗРК

4 Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК

Контрольные задания для СРС

1. К объектам информатизации, подлежащим обязательным испытаниям на соответствие требованиям ИБ, относят...

2. Испытания на соответствие требованиям ИБ включают следующие виды работ …

3. Лицензионные соглашения по критерию с кем и в каких целях заключаются делят на….

4. Составить 5 тестовых заданий различных форм по теме лекции

**Тема 2** Анализ предметной области и определение требований к ИС (3 часа)

План лекции

1. СТ РК 1090-2002 «Спецификация требований к программному обеспечению». IEEE 830-1998 «Методика составления спецификаций требований к программному обеспечению, рекомендуемая IEEE»
2. Открытый стандарт UML в анализе и проектировании программных систем.
3. СТ РК 34.015-2002 Техническое задание на создание автоматизированной системы

Для того чтобы разработать программную систему, приносящую реальные выгоды определенным пользователям, необходимо сначала выяснить, какие же задачи она должна решать для этих людей и какими свойствами обладать.

Требования к программным средствам определяют, какие свойства и характеристики оно должно иметь для удовлетворения потребностей пользователей и других заинтересованных лиц. В большинстве случаев будущие пользователи могут перечислить набор свойств, который они хотели бы видеть, но никто не даст гарантий, что это — исчерпывающий список.

Для выявления потребностей, а также для выяснения смысла высказанных требований приходится проводить достаточно большую дополнительную работу, которая называется анализом предметной области. В результате этой деятельности разработчики должны научиться понимать язык, на котором говорят пользователи и заказчики, выявить цели их деятельности, определить набор задач, решаемых ими.

Анализом предметной области занимаются системные аналитики или бизнес-аналитики, которые передают полученные ими знания другим членам проектной команды, сформулировав их на более понятном разработчикам языке. Для передачи этих знаний обычно служит некоторый набор моделей в виде графических схем и текстовых документов.

Важнейшие задачи функциональной диагностики организационных структур:

— классификация субъектов функционирования (категорий и групп работников);

— классификация элементов процесса функционирования (действий, процедур);

— классификация направлений (решаемых проблем), целей функционирования;

— классификация элементов информационных потоков;

— проведение обследования деятельности персонала организации;

— исследование распределения (по времени и частоте) организационных характеристик: процедур, контактов персонала, направлений деятельности, элементов информационных потоков — по отдельности и в комбинациях друг с другом по категориям работников, видам процедур и их направлениям (согласно результатам и логике исследований);

— выявление реальной структуры функциональных, информационных, иерархических, временных, проблемных отношений между руководителями, сотрудниками и подразделениями;

— установление структуры распределения рабочего времени руководителей и персонала относительно функций, проблем и целей организации;

— выявление основных технологий функционирования организации (информационных процессов, включая и недокументированные), их целеполагания в сравнении с декларируемыми целями организации;

— выявление однородных по специфике деятельности, целевой ориентации и реальной подчиненности групп работников, формирование реальной модели организационной структуры и сравнение ее с декларируемой.

Стандарт IEEE 830-1998 IEEE Recommended Practice for Software Requirements Specifications и СТ РК 1090-2002 ЕСПД «Спецификация требований к программному обеспечению» описывают рекомендуемые способы спецификации требований к программному обеспечению.

Результатом процесса спецификации требований является однозначно интерпретируемый и целостный документ-спецификация требований.

Стандарт на документальное оформление требований, задает определенные группировки одинаковых по своей сути требований (по их назначению), фиксируя классификацию требований.

Требования подразделяются на пользовательские и системные. Пользовательские требования – это описание на естественном языке (плюс поясняющие диаграммы) функций, выполняемых системой, и ограничений, накладываемых на неё. Системные требования – это описание особенностей системы (архитектура системы, требования к параметрам оборудования и т.д.), необходимых для эффективной реализации требований пользователя.

Разработка требований — это процесс, включающий мероприятия, необходимые для создания и утверждения документа, содержащего спецификацию системных требований. Различают четыре основных этапа процесса разработки требований:

— анализ технической осуществимости создания системы,

— формирование и анализ требований,

— специфицирование требований и создание соответствующей документации,

— аттестация (тестирование) этих требований.

Пользовательские требования должны описывать внешнее поведение системы, основные функции и сервисы, предоставляемые системой, её нефункциональные свойства. Пользовательские требования можно оформить как простым перечислением, так и используя нотацию вариантов использования.

Пользовательские требования оформляются в виде вариантов использования (use cases), пользовательских историй (user stories), пользовательских сценариев (user scenarios).

Вариант использования (use case) продукта описывает последовательность взаимодействия системы и внешнего действующего лица. Действующим лицом (actor) может быть человек, другая система ПО или аппаратное устройство, взаимодействующее с системой для достижения некой цели.

Существует несколько сценариев варианта использования.

Один сценарий считается нормальным направлением развития (normal course) варианта использования, его также называют основным направлением, базовым направлением, нормальным потоком, основным сценарием, главным успешным сценарием и благоприятным путем.

Другие допустимые сценарии из варианта использования, называются альтернативными направлениями (alternative courses) или вторичными сценариями (secondary scenarios). Они также могут привести к успешному выполнению задания и удовлетворяют выходным условиям варианта использования. Однако они представляют вариации решения задачи или диалоговой последовательности, необходимой для выполнения задачи. В определенной точке принятия решений в диалоговой последовательности нормальное направление может перейти в альтернативное, а затем вернуться обратно в нормальное. Условия, препятствующие успешному завершению задания, называются исключениями (exceptions).

Диаграмма UML вариантов использования может содержать следующие виды элементов:

- актор (Actor), который графически отображается в виде фигуры «человечка» под которой записывается имя актора;

- вариант использования (Use Case), который графически отображается в виде эллипса, под которым записывается имя. Прецедент – это то, что должна делать система по желанию конкретного актера, всегда инициируются актером, всегда описываются с точки зрения актеров.

- примечание (Note), которое может быть привязано к любому объекту диаграммы. Графически оно отображается в виде прямоугольника с «загнутым» правым уголком, внутри которого записывается текст примечания;

- отношение ассоциации (Association), которое графически отображается в виде сплошной линии;

- отношение наследования или обобщения (Generalization), которое графически отображается в виде сплошной линии со стрелкой в виде незакрашенного треугольника;



- отношение зависимости или реализации (Dependency or instantiates), которое графически отображается в виде пунктирной линии со стрелкой на конце;

- якорь для замечания (Note Anchor), который позволяет соединить элемент Note с любым элементом на диаграмме. Графически отображается в виде пунктирной линии без стрелки.

Элементы на диаграмме могут располагаться на любом месте.

Диаграмма UML деятельности. Данный тип диаграмм может использоваться для отражения последовательности действий (элементарных операций) во время выполнения некоторого бизнес-процесса, представленного на диаграмме вариантов использования. Традиционно для этой цели использовались блок-схемы или структурные схемы алгоритмов.

Графически диаграмма деятельности представляется в форме графа, вершинами которого являются действия (операции, шаги процесса), а дугами – переходы от одного действия к другому. На диаграмме можно также отразить ветвление, т.е. возможность перехода к различным действиям в зависимости от некоторых условий.

Начальное состояние (Start State), соответствующее началу процесса, обозначается в виде закрашенного кружка; конечное состояние (End State), соответствующее завершению процесса – в виде закрашенного кружка, помещенного в окружность.

Действие (activity) изображается фигурой, напоминающей прямоугольник с закругленными сторонами, внутри которого записывается выражение действия.

Переход (Tranzition) изображается сплошной линией со стрелкой.

Если после выполнения некоторого действия процесс должен разделиться на альтернативные ветви в зависимости от некоторого условия, то ставится знак ветвления (Desizion) в виде ромба, внутри которого нет никакого текста. В него может входить только одна стрелка. Выходящих стрелок может быть две или более. Для каждой из них указывается соответствующее условие, при котором выполняется данный переход.

В РК действует ГОСТ СТ РК 34.015-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы», который рекомендует следующие разделы, которые могут быть разделены на подразделы:

- общие сведения;

- назначение и цели создания (развития) системы;

- характеристика объектов автоматизации;

- требования к системе;

- состав и содержание работ по созданию системы;

- порядок:

1) контроля и приемки системы;

2) порядок оформления и предъявления заказчику результатов работ по созданию системы (ее части), по изготовлению наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы;

- требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие;

- требования к документированию;

- источники разработки.

Подраздел «Требования к системе в целом» содержит требования к защите информации от несанкционированного доступа; требования по сохранности информации при авариях; требования к защите от влияния внешних воздействий.

В требования к защите информации от несанкционированного доступа включают требования, установленные в НТД (нормативно-технической документации), действующей в отрасли (ведомстве) заказчика.

В требованиях по сохранности информации приводят перечень событий: аварий, отказов технических средств (в том числе - потеря питания) и т. п., при которых должна быть обеспечена сохранность информации в системе.

В требованиях к средствам защиты от внешних воздействий приводят:

- требования к радиоэлектронной защите средств АС;

- требования по стойкости, устойчивости и прочности к внешним воздействиям (среде применения).

В ТЗ на АС могут включаться приложения.

Как правило, техническое задание составляется компанией ‐ будущим разработчиком ‐ после проведения интервью с заказчиком. В ходе интервью (одной или ряда встреч), представители разработчика выясняют те моменты, которые затем найдут отражение в документе. На интервью со стороны заказчика желательно присутствие всех заинтересованных в создании и всех, кто будет причастен к его исполнению.

Если в компании‐заказчике есть грамотные IT‐специалисты, то их следует привлечь к согласованию ТЗ. Если же ситуация иная, а речь идет о крупном проекте, бывает целесообразно привлечение независимого эксперта в качестве консультанта, который оценит качество и полноту составления технического задания и защитит интересы заказчика.

Основные этапы подготовки технического задания:

1. Описание предметной области:

— Краткое введение в предметную область

— Выделить элементы предметной области, их взаимосвязи

— Определить особенности и ограничения предметной области

— Используемые термины и сокращения

2. Цель создания системы:

— Сформулировать цель создания системы – как ответ на вопрос что за процесс в предметной области будет автоматизирован

— Назначение системы, существующие аналоги

— Целевая аудитория, ожидаемый уровень использования

3. Детализация функций системы:

— Изучение потребностей заказчика

— Подготовить описание функций системы

4. Анализ категорий пользователей:

— Выделение категорий пользователей

— Определение функциональных требований пользователей каждой категории

5. Определение ограничений:

— Анализ аппаратных особенностей и ограничений

— Анализ топологии и особенностей развертывания

— Определение технологических ограничений

6. Формирование и утверждение совокупного списка требований к системе:

— Если система предполагает интерактивность в общении с пользователем, то определить функциональные требования (описывают в динамике сценарии взаимодействия посетителя с системой) и структуру данных.

— Выделить специфические требования (например, многоязычность, требования к дизайну экранов оператора)

— Прочие требования (например, какая документация должна быть предоставлена разработчиком)

— Сформировать список требований

7. Выработка архитектурного решения

— Выбор технологической платформы

— Если система должна реализовывать специфическую бизнес‐логику, в которой обычно хорошо разбирается заказчик и плохо ‐ исполнитель, эта логика должна быть задокументирована в техническом задании максимально подробно.

— Подготовка модульной структуры системы

— Подготовка детализированного описания подсистем

8. Подготовка календарного плана

— Оценка сложности реализации подсистем.

— Выделение работ, построение сетевого графика.

— Оценка сроков выполнения работ.

9. Завершающий этап

— Согласование процесса приемки работ

— Компоновка из полученных материалов текста технического задания

Настоящий стандарт устанавливает состав, содержание, правила оформления документа «Техническое задание на создание (развитие или модернизацию) системы». Требования настоящего стандарта являются обязательными.

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 июня 2019 года № 143/НҚ Об утверждении Правил составления и рассмотрения технических заданий на создание и развитие объектов информатизации "электронного правительства".

Также в техническом задании указываются сведения о классе объекта информатизации, архитектуре объекта информатизации, сетевой инфраструктуре и развертывании проекта. Результаты классификационной оценки ИС определяются на основе Классификатора объектов информатизации и в соответствии с Правилами классификации объектов информатизации, утвержденными приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135. https://adilet.zan.kz/rus/docs/V1600013349#z4

Рекомендуемая литература

1 Стандарт IEEE 830-1998 «Методика составления спецификаций требований к программному обеспечению, рекомендуемая IEEE»

2 СТ РК 1090-2002 ЕСПД. «Спецификация требований к программному обеспечению».

3 СТ РК 34.015-2002 Техническое задание на создание автоматизированной системы

4 Приказ «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации» и.о. Министра по инвестициям и развитию РК от 28 января 2016 года № 135

5 Буч Г., Рамбо Д., Якобсон И. Язык UML. Руководство пользователя. 2-е изд.: Пер. с англ –М.: ДМК Пресс, 2014

Контрольные задания для СРС

1. Что является результатом этапа системного анализа предметной области?

2. Какие бывают уровни представления требований?

3. К какому стандарту относится модель вариантов использования?

4. Какими СТ РК и руководящими документами нужно руководствоваться при написании раздела «Требования к документированию»?

5. Составить 5 тестовых заданий различных форм по теме лекции

**Тема 3** Управление рисками ИБ (3 часа)

План лекции

1. Риск-ориентированный подход
2. Постановление Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».
3. СТ РК ИСО/МЭК 31010 «Менеджмент риска. Методы оценки рисков»; СТ РК ИСО/МЭК 27005 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности»
4. Формирование каталога угроз (рисков) ИБ; Методика оценки рисков; Разработка плана обработки угроз

Основные нормативные правовые акты и национальные стандарты Республики Казахстан применяемые оценке рисков:

* постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
* государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 31010-2020 «Менеджмент риска. Методы оценки рисков»;
* национальный стандарт Республики Казахстан СТ РК ИСО/МЭК 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».

Любая компания, вне зависимости от уровня своей зрелости, обладает какой-либо чувствительной информацией, нелегитимная манипуляция которой может привести к прямым или косвенным финансовым потерям.

Целью анализа рисков, связанных с обладанием чувствительной информацией и эксплуатацией информационных систем (ИС), является оценка угроз (т. е. условий и факторов, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также ее доступности) и уязвимостей (слабых мест в защите, которые делают возможной реализацию угрозы), а также определение комплекса контрмер, обеспечивающего достаточный уровень защищенности ИС -  риск-ориентированный подход (или риск-менеджмент). Суть подхода — решения по реализации мер защиты информационной системы принимаются на основе анализа и оценки рисков нанесения ущерба организации.

С целью управления рисками осуществляются:

1) выбор методики оценки рисков в соответствии с рекомендациями стандарта Республики Казахстан СТ РК 31010 "Менеджмент риска. Методы оценки риска" и разработка процедуры анализа рисков;

2) идентификация рисков в отношении перечня идентифицированных и классифицированных активов, включающая:

* выявление угроз ИБ и их источников;
* выявление уязвимостей, которые могут привести к реализации угроз;
* определение каналов утечки информации;
* формирование модели нарушителя;

3) выбор критериев принятия идентифицированных рисков;

4) формирование каталога угроз (рисков) ИБ, включающего оценку (переоценку) идентифицированных рисков в соответствии с требованиями стандарта Республики Казахстан СТ РК ISO/IEC 27005 "Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности".

5) разработка и утверждение плана обработки угроз (рисков) ИБ, содержащего мероприятия по их нейтрализации или снижению.

Объектами, в отношении которых осуществляется внедрение комплекса мер управлению рисками ИБ, могут выступать:

1) имущественные активы (объекты информатизации) такие как:

* информация (файлы данных, базы данных, документы) хранимая, обрабатываемая, передаваемая;
* программные активы (прикладное, общесистемное, специализированное ПО, инструментальные средства разработки и утилиты);
* физические активы (компьютерное и телекоммуникационное оборудование, аппаратура связи, сменные носители информации и другое оборудование);
* услуги (бизнес-процессы и сервисы);
* люди (персонал, пользователи);

2) нематериальные активы (репутация, имидж Товарищества).

Процесс управления рисками ИБ состоит из следующих логических этапов:

1) определение организационной структуры управления рисками ИБ, области применения, границ и основных критериев;

2) идентификация и анализ рисков ИБ;

3) оценивание (ранжирование) рисков ИБ;

4) принятие решения и разработка плана реагирования на риски ИБ;

5) реализация мероприятий по реагированию на риски ИБ и контроль их исполнения;

6) мониторинг и переоценка рисков ИБ, оценка эффективности реализованных мер по обеспечению ИБ.

Определение границ и области применения управления рисками ИБ осуществляется с целью выявления среды, в которой производится управление рисками ИБ и всех значимых активов, которые бы принимались в расчет при оценке рисков.

Должны быть разработаны и определены критерии, используемые при управлении рисками, такие как критерии оценивания риска, критерии влияния (воздействия) последствий от реализации риска, критерии принятия риска.

Критерии оценивания рисков могут использоваться для определения приоритетов при обработке рисков.

Критерии влияния (воздействия) последствий идентифицируются с возможной утратой конфиденциальности, целостности и доступности активов и отражают неблагоприятное изменение уровня достигнутых бизнес-целей.

Критерии принятия риска определяют максимально допустимый уровень остаточного риска, а также возможные исключения для определенных рисков при определенных обстоятельствах. Необходимо определить шкалы для уровней риска

Идентификация риска представляет собой процесс определения элементов риска, составления их перечня и описания каждого из элементов риска.

В рамках идентификации риска необходимо осуществить:

* идентификацию активов;
* идентификацию угроз;
* идентификацию уязвимостей;
* идентификацию имеющихся в Организации и применяемых защитных механизмов и средств;
* идентификацию последствий инцидентов ИБ.

В пределах установленной области и границ применения активы должны быть выявлены и по результатам их идентификации должен быть составлен реестр активов.

Для каждого актива должен быть определен владелец, чтобы обеспечить учёт и ответственность за каждый актив. Владелец актива несет ответственность за его использование и безопасность. Чаще всего владелец актива является наиболее подходящим лицом, способным определить реальную ценность актива.

Идентификация активов должна осуществляться на уровне детализации, обеспечивающем достаточную информацию для оценки рисков ИБ.

Следующим шагом после выявления активов является определение его ценности.

При количественном подходе к оценке рисков ценность активов определяется в денежном выражении.

При качественном подходе к оценке рисков ценность актива можно определить по уровню критичности (последствиям) при нарушении характеристик безопасности (конфиденциальность, целостность, доступность) актива на основании разработанной шкалы, которая может иметь разное количество значений.

Выявленные угрозы должны быть соотнесены с активами. Некоторые угрозы (риски) могут влиять более чем на один актив.

Целью идентификации уязвимостей является составление перечня уязвимостей актива.

Уязвимости могут быть связаны со свойствами актива, которые могут использоваться способом и целью, отличающимися от тех, которые планировались при приобретении или создании актива.

Идентификация последствий инцидентов ИБ заключается в составлении перечня сценариев инцидентов ИБ с их последствиями для Организации.

В ходе идентификации необходимо проанализировать для активов последствия, которые могут быть результатом потери конфиденциальности, целостности и доступности. Такими последствиями могут стать потеря эффективности, неблагоприятные операционные условия функционирования, неработоспособность бизнес-процесса, репутационные потери, упущенные возможности, потери рабочего времени и так далее.

Последствие инцидентов ИБ может затронуть один актив, часть актива или несколько активов.

Применяемые средства защиты могут быть оценены как эффективные, неэффективные, недостаточные или необоснованные.

Если средство защиты посчитали недостаточным или необоснованным, необходимо принять решение, стоит ли его удалить, заменить другим более подходящим или продолжить его применять, например, по стоимостным причинам.

Анализ рисков представляет собой процесс изучения характера риска и определение его уровня.

В рамках анализа рисков ИБ необходимо:

* оценить тяжесть влияния (воздействия) последствий от реализации рисков ИБ;
* оценить вероятность возникновения (реализации) риска ИБ;
* измерять уровень риска.

Каталог угроз (рисков) ИБ рассматривается на совещании рабочей группы или ответственного за управление рисками ИБ с руководством Организации и руководителями структурных подразделений Организации и утверждается первым руководителем Организации.

Оценивание (ранжирование) рисков представляет собой процесс сопоставления уровня риска с критериями принятия риска, установленными в Организации для процесса управления рисками. Принимаемые на данном этапе решения включают в себя, как правило, вопросы необходимости обработки риска и расстановки приоритетов обработки риска.

Для Организации установлены следующие приемлемые уровни риска - очень низкий и низкий.

Умеренные, высокие и очень высокие риски требуют обработки.

На выходе процесса оценивания (ранжирования) рисков ИБ должна быть сформирована карта рисков.

Обработка риска ИБ представляет собой процесс модификации риска посредством выбора соответствующего варианта его обработки и расчета остаточного риска.

Существует четыре основных варианта обработки риска:

* снижение риска;
* сохранение риска;
* избегание риска;
* передача риска.

Четыре варианта обработки рисков не являются взаимоисключающими. Организации может их объединять.

Планируемые мероприятия по обработке риска дают возможность рассчитать ожидаемый уровень риска.

Принятое по каждому риску решение должно быть зафиксировано в Плане обработки рисков информационной безопасности

Обмен информацией относительно рисков ИБ - процесс, направленный на достижение целей в области управления рисками ИБ путем обмена и/или совместного использования информации о рисках между лицами, принимающими решения и другими причастными сторонами. Информация включает (но не ограничивается) наличие, характер, форму, вероятность, серьезность, обработку и приемлемость рисков ИБ.

Необходимо разработать и утвердить регламент взаимодействия по рискам ИБ в обычных и нештатных ситуациях, поскольку данная деятельность должна осуществляться непрерывно. Этот регламент должен включать в себя механизмы для регулярного обновления информации о рисках ИБ как составной части программы непрерывного повышения осведомленности сотрудников Товарищества в вопросах ИБ. Он также должен предусматривать оповещение причастных лиц об инцидентах ИБ.

Рекомендуемая литература

1 СТ РК ISO/IEC 27005-2013 Информационные технологии Методы обеспечения безопасности. Менеджмент риска информационной безопасности

2 СТ РК ISO/IEC 31010-2020 Менеджмент риска. Методы оценки риска

3 Постановление Правительства РК «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» от 20 декабря 2016 года № 832

Контрольные задания для СРС

1. Для чего нужны законодательные меры в области информационной безопасности?

2. Какими документами регулируется информационная безопасность в РК?

3. Какие основополагающие документы в области информационной безопасности вам известны?

4. Что понимается под термином информационный объект?

5. Что представляет собой угроза права собственности?

6. Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?

7. Составить 5 тестовых заданий различных форм по теме лекции

**Тема 4** Стандарты ИБ серия 27000 (3 часа)

План лекции

1. СТ РК ISO/IEC 27000 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь.
2. СТ РК ISO/IEC 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования
3. СТ РК ISO/IEC 27002 Информационная технология Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации.
4. СТ РК ISO/IEC 27003 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности.
5. . СТ РК ISO/IEC 27004 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерение.

Ведущей организацией, разрабатывающей международные стандарты и документы в области защиты информации в рамках совместного технического комитета ISO/IEC JTC 1 «Информационные технологии», является его структурное подразделение – технический подкомитет ISO/IEC JTC 1/SC 27 «Информационная безопасность, кибербезопасность и защита конфиденциальности» (jtc1info.org).

По основным направлениям стандартизации в структуре ISO/IEC JTC 1/SC 27 функционируют пять рабочих групп, каждая из которых отвечает за разработку проектов стандартов и их техническое содержание.

Стандарты Республики Казахстан при обеспечении ИБ включают в себя семейство стандартов 27000, определяющее требования к системам управления информационной безопасностью и к сертификации таких систем.

В настоящее время серия 27xxx содержит более 40 стандартов по различным направлениям информационной безопасности, начиная с уровня стратегического управления и контроля системы менеджмента ИБ и заканчивая техническими рекомендациями по применению отдельных программно-технических и организационных мер защиты информации. https://adilet.zan.kz/rus/docs/H19RK000009 (Перечень стандартов и рекомендаций).

Базовые стандарты ISO/IEC 27001 и ISO/IEC 27002 со временем были дополнены следующими документами:

* стандартом ISO/IEC 27000, описывающим терминологию и общий подход всей серии стандартов;
* стандартом ISO/IEC 27003 с указаниями по порядку внедрения СМИБ;
* стандартами по отдельным процессам СМИБ: измерению эффективности, риск-менеджменту, аудиту;
* стандартами по направлениям стратегического управления ИБ и экономике СМИБ;
* стандартами по особенностям СМИБ в специфических областях деятельности: телекоммуникационных услугах, финансовых операциях, обработке персональных данных в облачных сервисах, топливно-энергетическом комплексе, сообществах информационного обмена, организациях здравоохранения;
* детальными требованиями к мерам защиты информации, в том числе по управлению инцидентами, сетевой безопасности;
* руководствами по интеграции СМИБ с системами ИТ-менеджмента (ISO 20000) и системами обеспечения непрерывности деятельности (в том числе ISO 22301);
* руководством по обеспечению кибербезопасности в соответствии с общим подходом и практиками СМИБ;
* стандартами ISO/IEC 27006 и ISO/IEC 27021, описывающим требования к экспертам и аудиторам СМИБ.

ISO/IEC 27000 – комплекс стандартов СМИБ, содержащий требования к СМИБ и к органам, сертифицирующим такие системы, управлению рисками, метрикам и измерениям, а также руководство по внедрению СМИБ в организации.

ISO/IEC 27000 содержит общий обзор систем менеджмента информационной безопасности (СМИБ).

Термины и определения, представленные в стандарте ISO/IEC 27000:

- охватывают общие термины и определения, используемые в семействе стандартов СМИБ;

- не охватывают все термины и определения, применяемые в семействе стандартов СМИБ;

- не ограничивают применение новых терминов в семействе стандартов СМИБ.

ISO/IEC 27000 применим к организациям любого типа и размера (коммерческим предприятиям, правительственным учреждениям, некоммерческим организациям).

ISO/IEC 27001 устанавливает требования к СМИБ и используется для целей сертификации. ISO/IEC 27552 конкретизирует 27001 и охватывает процессы защиты сбора, учета, доступности, целостности и конфиденциальности данных (первый международный стандарт по решению вопросов управления конфиденциальной информацией) .

Соответствие стандарту ISO/IEC 27001 означает, что организация или предприятие внедрило систему управления рисками, связанными с безопасностью данных, принадлежащих компании или обрабатываемых ею, и что в этой системе соблюдены все лучшие практики и принципы, закрепленные в данном международном стандарте.

Принципы ИБ в ISO/IEC 27001

Конфиденциальность - только определенный круг людей может получить доступ к информации, хранящейся в организации. ⚠ Пример риска: Преступники завладели регистрационными данными ваших клиентов и продают их в даркнете.

Целостность информации - данные, которые организация использует для ведения своего бизнеса или хранит для других, надежно хранятся, не стираются и не повреждаются никоим образом. ⚠ Пример риска: Сотрудник случайно удаляет строку в файле во время его обработки.

Доступность данных - организация и ее клиенты имеют возможность доступа к информации, когда это необходимо, для удовлетворения деловых целей и ожиданий клиентов. ⚠ Пример риска: База данных вашего предприятия выходит из строя из-за проблем с сервером и недостаточного резервного копирования.

СМИБ, отвечающая требованиям стандарта ISO/IEC 27001, сохраняет конфиденциальность, целостность и доступность информации путем применения процесса управления рисками и дает уверенность заинтересованным сторонам в том, что риски адекватно управляются.

ISO/IEC 27002 содержит рекомендации по созданию и практическому использованию в организации СМИБ, включая вопросы выбора, внедрения и применения полноценного набора мер обеспечения ИБ, соответствующих совокупности имеющихся в данной организации рисков ИБ.

Стандарт предназначен для использования организациями:

* в качестве справочного материала при выборе мер обеспечения информационной безопасности (ИБ) в процессе внедрения СМИБ на основе ИСО/МЭК 27001 или в качестве руководства для организаций, реализующих общепринятые меры обеспечения ИБ.
* при разработке отраслевых руководств и руководств для конкретных организаций по менеджменту информационной безопасности с учетом характерных для них рисков ИБ.

ISO/IEC 27003 содержит руководство по реализации требований к СМИБ, приведенных в ISO/IEC 27001, и предоставляет рекомендации (используя вспомогательный глагол "должен"), возможности (используя вспомогательный глагол "следует") и допустимое действие (используя вспомогательный глагол "может") в отношении этих требований. Настоящий стандарт не ставит целью предоставление общего руководства по всем аспектам ИБ.

ISO/IEC 27003 является базовым и всеохватывающим документом, содержит разъяснения и руководство по ISO/IEC 27001, но не содержит подробных описаний, касающихся "мониторинга, измерения, анализа и оценки" и управления рисками ИБ.

ISO/IEC 27003 носит общий характер и предназначен для применения во всех организациях, независимо от их типа, размера или характера. Организация определяет, какая часть этого руководства применяется к ней в соответствии с конкретным контекстом организации.

ISO/IEC 27004 представляет руководящие принципы, предназначенные для оказания помощи организациям в оценке деятельности по обеспечению информационной безопасности и результативности системы менеджмента информационной безопасности (СМИБ) в целях выполнения требований, изложенных в подразделе 9.1 ISO/IEC 27001.

ISO/IEC 27004 охватывает:

-мониторинг и оценку деятельности по обеспечению ИБ;

-мониторинг и оценку результативности системы менеджмента информационной безопасности (СМИБ), включая ее процессы и средства контроля и управления;

-анализ и оценку результатов мониторинга и оценки защищенности.

ISO/IEC 27004 применим для всех организаций, независимо от типа или размера.

ISO/IEC 27005 представляет руководство по менеджменту риска информационной безопасности в организации, поддерживая, в частности, требования к системе менеджмента информационной безопасности (СМИБ) в соответствии с ISO/IEC 27001.

ISO/IEC 27005 поддерживает общие концепции, определенные в ISO/IEC 27001, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска.

ISO/IEC 27005 не предоставляет какой-либо конкретной методологии по менеджменту риска информационной безопасности. Выбор подхода к менеджменту риска осуществляется организацией и зависит, от области применения СМИБ, контекста менеджмента риска или сферы деятельности.

ISO/IEC 27005 применим для организаций всех типов (например, коммерческих предприятий, государственных учреждений, некоммерческих организаций), планирующих осуществлять менеджмент рисков, которые могут скомпрометировать информационную безопасность организации.

ISO/IEC 27005 предназначен для руководителей и персонала, занимающегося в организации вопросами менеджмента риска информационной безопасности, а также, при необходимости, для внешних сторон, имеющих отношение к этому виду деятельности.

ISO/IEC 27002 содержит рекомендации по созданию и практическому использованию в организации системы менеджмента информационной безопасности (СМИБ), включая вопросы выбора, внедрения и применения полноценного набора мер обеспечения ИБ, соответствующих совокупности имеющихся в данной организации рисков ИБ.

ISO/IEC 27002 состоит из 14 разделов, содержащих в совокупности 114 конкретных мер обеспечения ИБ, сгруппированных в 35 основных категорий. Каждый раздел, посвященный мерам обеспечения ИБ, содержит описание одной или нескольких основных категорий.

В зависимости от обстоятельств меры обеспечения ИБ из одного или всех разделов могут быть применимы, поэтому каждая организация при использовании настоящего стандарта должна определить важность и применимость мер для себя и отдельных бизнес-процессов.

Порядок следования разделов не отражает их важности, не предполагает распределения их по приоритету.

Каждая основная категория содержит:

a) цель применения мер, которая содержит описание того, что должно быть достигнуто;

b) одну или несколько мер обеспечения ИБ, которые могут быть применены для достижения цели применения меры.

Описание меры обеспечения ИБ структурировано следующим образом:

Мера обеспечения ИБ определяет конкретную формулировку меры, направленную на достижение цели применения меры.

Руководство по применению предоставляет более подробную информацию для помощи в реализации меры и достижения целей управления. Руководство может не совсем подходить или быть недостаточным для всех ситуаций и может не соответствовать специфичным требованиям организации к мере обеспечения ИБ.

Дополнительная информация, которую следует принять во внимание, например, вопросы юридического характера или ссылки на другие стандарты. Если дополнительной информации нет, то эта часть отсутствует.

Рекомендуемая литература

1 СТ РК ISO/IEC 27005-2013 Информационные технологии Методы обеспечения безопасности. Менеджмент риска информационной безопасности

2 СТ РК ISO/IEC 31010-2020 Менеджмент риска. Методы оценки риска

3 СТ РК ISO/IEC 27000-2019 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь

4 СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования

5 СТ РК ISO/IEC 27002-2015 Информационная технология Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации

6 СТ РК ISO/IEC 27003-2018 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности

7 СТ РК ISO/IEC 27004-2018 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерение.

Контрольные задания для СРС

1. Рекомендации по созданию и практическому использованию в организации СМИБ, включая вопросы выбора, внедрения и применения полноценного набора мер обеспечения ИБ представлены в стандарте…

2. Какой стандарт содержит разъяснения и руководство по стандарту ISO/IEC 2700?

3. Какой стандарт представляет руководящие принципы, предназначенные для оказания помощи организациям в оценке деятельности по обеспечению информационной безопасности и результативности системы менеджмента информационной безопасности (СМИБ)?

4. Какой принцип ИБ в ISO/IEC 27001 соответствует формулировке «Только определенный круг людей может получить доступ к информации, хранящейся в организации»?

5. В какой части описания меры (ISO/IEC 27002) содержится подробная информацию для помощи в реализации меры и достижения целей управления?

6. Составить 5 тестовых заданий различных форм по теме лекции

**Тема 5** Технология сертификации средств ИБ (3 часа)

План лекции

1. Проведение испытаний объектов информатизации на соответствие требованиям информационной безопасности.
2. СТ РК ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий
3. Оценочный уровень доверия
4. Реестр доверенного программного обеспечения и продукции электронной промышленности

Нормативно правовые акты и стандарты РК:

1. Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V.

2. Закон РК «О связи»  от 5 июля 2004 года N 567.

3. Постановление Правительства РК от 20 декабря 2016 года № 832 «Об утверждении единых требований в области  информационно-коммуникационных технологий и обеспечения информационной безопасности»

4. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности РК «Об утверждении методики и правил проведения испытаний объектов информатизации "электронного правительства" и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности». Порядок и схемы проведения сертификации

5. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации».

6. СТ РК ИСО/МЭК 15408-2017 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Часть 2. Функциональные требования безопасности Часть 3. Требования к обеспечению защиты»;

7. СТ РК ИСО/МЭК 13335-5-2008 «Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 5. Руководство по управлению защитой сети»;

8. СТ РК ISO/IEC 27001-2015 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью»;

9. СТ РК ISO/IEC 27002-2015 «Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасности».

Проведение испытания включает:

1) анализ исходных кодов;

2) испытание функций информационной безопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры;

5) обследование процессов обеспечения информационной безопасности.

Анализ исходных кодов проводится с целью выявления недостатков программного обеспечения, осуществляется в следующем порядке:

1) проводится подготовка исходных данных (загрузка исходных кодов объектов информатизации), выбор режима сканирования (динамический и/или статический), настройка характеристик режимов сканирования;

2) запускается программное средство, предназначенное для выявления недостатков ПО;

3) проводится анализ программных отчетов на наличие ложных срабатываний;

4) формируется отчет, включающий в себя перечень выявленных недостатков ПО с указанием их описания, маршрута (пути к файлу) и степени риска (высокая, средняя, низкая).

Объем работ по анализу исходного кода определяется размером исходного кода. Результаты анализа исходных кодов фиксируются в протоколе анализа исходных кодов.

Испытание функций информационной безопасности осуществляется с целью оценки их соответствия требованиям технической документации, нормативных правовых актов РК и действующих на территории РК стандартов в сфере информационной безопасности, включает:

1) оценку соответствия функций безопасности серверов и виртуальных ресурсов, в том числе с применением программных средств (при необходимости);

2) фиксацию результатов испытания с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости).

Перечень функций информационной безопасности приведен в приложении 1 к Методике.

Результаты испытаний функций информационной безопасности фиксируются в протоколе испытаний функций информационной безопасности.

Нагрузочное испытание проводится с целью оценки соблюдения доступности, целостности и конфиденциальности объекта испытаний, с использованием специализированного программного средства на основании автоматических сценариев, в среде штатной эксплуатации объекта испытаний, в которой персональные данные заменены на фиктивные.

При проведении нагрузочного испытания выявляются параметры фактической нагрузочной способности объекта испытаний.

Нагрузочное испытание осуществляется в следующем порядке:

1) проводится подготовка к испытанию;

2) проводится испытание;

3) фиксируются результаты испытания.

Подготовка к испытанию включает:

1) определение сценария испытания;

2) определение временных и количественных характеристик испытания;

3) согласование времени проведения испытания c заказчиком.

Проведение испытания включает:

1) настройка конфигурации и сценария испытания в специализированное программное средство;

2) запуск специализированного программного средства;

3) регистрация нагрузки на объект испытаний;

4) формирование отчета с указанием рекомендаций по увеличению или снижению реальной пропускной способности объекта испытаний.

Работы проводятся по количеству вариантов точек подключений пользователей и вариантов точек подключения интеграционного взаимодействия объекта испытаний.

Результаты нагрузочного испытания фиксируются в протоколе нагрузочного испытания.

Обследование сетевой инфраструктуры проводится с целью оценки безопасности сетевой инфраструктуры, включает:

1) оценку соответствия функций защиты сетевой инфраструктуры требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информационной безопасности;

2) обследование сетевой инфраструктуры заявителя, в том числе с применением программных средств (при необходимости);

3) сканирование программным средством на наличие известных уязвимостей программного обеспечения из базы общих уязвимостей и рисков;

4) фиксацию полученных результатов испытания в отчете с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости).

Перечень функций защиты сетевой инфраструктуры приведен в приложении 2 к Методике.

Работы по обследованию сетевой инфраструктуры, проводятся для каждого сегмента сети (подсети) объекта испытаний.

Результаты обследования сетевой инфраструктуры фиксируются в протоколе обследования сетевой инфраструктуры.

Обследование процессов обеспечения информационной безопасности осуществляется с целью определения их соответствия требованиям нормативных правовых актов и стандартов в сфере обеспечения информационной безопасности, включает:

1) оценку соответствия процессов обеспечения информационной безопасности требованиям нормативных правовых актов и стандартов в сфере обеспечения информационной безопасности;

2) фиксацию результатов оценки испытания с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости);

3) сканирование серверов, виртуальных ресурсов и сетевого оборудования программными средствами на наличие известных уязвимостей;

4) анализ выявленных уязвимостей на наличие ложного срабатывания и формирование рекомендаций по их устранению в зависимости от степени их критичности (при необходимости).

Перечень процессов обеспечения информационной безопасности и их содержание приведено в приложении 3 к Методике.

Результаты обследования процессов обеспечения информационной безопасности фиксируются в протоколе обследования процессов обеспечения информационной безопасности.

Все объекты информатизации проходят этапы создания, опытной и промышленной эксплуатации, развития и прекращения его использования. Это касается и информационных систем, которые перед вводом в промышленную эксплуатацию в обязательном порядке проходят процедуру испытаний на соответствие требованиям информационной безопасности.

Субъекты квазигосударственного сектора - государственные предприятия, товарищества с ограниченной ответственностью, акционерные общества, в том числе национальные управляющие холдинги, национальные холдинги, национальные компании, учредителем, участником или акционером которых является государство, а также дочерние, зависимые и иные юридические лица, являющиеся аффилиированными с ними в соответствии с законодательными актами Республики Казахстан; Ст. 3 Бюджетный кодекс РК.

Субъекты:

* Государственные органы
* Местные исполнительные органы
* Государственные юридические лица
* Квазигосударственный сектор
* КВОИКИ (критически важные объекты информационно-коммуникационной инфраструктуры)

В соответствие с пунктом 2 статьи 49 Закона РК «Об информатизации», к объектам испытаний, подлежащим обязательным испытаниям на соответствие требованиям ИБ, относятся:

* программное обеспечение (программный продукт), созданное и (или) размещенное на информационно-коммуникационной платформе «электронного правительства»;
* информационно-коммуникационная платформа «электронного правительства»;
* интернет-ресурс государственного органа, государственного юридического лица, субъекта квазигосударственного сектора;
* информационная система государственного органа, государственного юридического лица, субъекта квазигосударственного сектора;
* критически важные объекты информационно-коммуникационной инфраструктуры;
* негосударственная информационная система, предназначенная для формирования государственных электронных информационных ресурсов, осуществления государственных функций и оказания государственных услуг.

Испытания объектов информатизации «электронного правительства» на соответствие требованиям информационной безопасности проводит Государственная техническая служба, интернет-портал SYNAQ – интернет-портал государственной технической службы, предназначен для автоматизации процесса оказания услуги по испытаниям объектов информатизации «электронного правительства».

Испытания на соответствие требованиям информационной безопасности информационной системы, отнесенной к критически важным объектам информационно-коммуникационной инфраструктуры (за исключением являющихся объектами информатизации «электронного правительства»), проводятся аккредитованными испытательными лабораториями.

Акт по результатам испытаний на соответствие требованиям информационной безопасности выдается уполномоченным органом.

СТ РК ISO/IEC 15408-2017 состоит из трех частей:

- СТ РК ISO/IEC 15408-1 (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель) - устанавливает общий подход к формированию требований и оценке безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии Общих критериев определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

- СТ РК ISO/IEC 15408-2 (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности) содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

- СТ РК ISO/IEC 15408-3 (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты) включает в себя систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

Стандарт устанавливает требования доверия ISO/IEC 15408 и включает оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия для ОО-компонентов, составные пакеты доверия (СоПД), определяющие шкалу для измерения доверия для составных ОО (объект оценки), отдельные компоненты доверия, из которых составлены уровни и пакеты доверия, а также критерии для оценки профилей защиты (ПЗ) и задания по безопасности (ЗБ).

Доверие - основа для уверенности в том, что продукт ИТ отвечает целям безопасности.

Наиболее обобщенная совокупность требований доверия называется классом. Каждый класс содержит семейства доверия, которые разделены на компоненты доверия, содержащие, элементы доверия. Классы и семейства используются для обеспечения систематизации классифицируемых требований доверия, в то время как компоненты применяются для спецификации требований доверия в ПЗ/ЗБ.

Основная концепция - это обеспечение доверия, основанное на оценке (активном исследовании) продукта ИТ, который должен соответствовать определенным критериям безопасности.

Оценочные уровни доверия (ОУД) образуют возрастающую шкалу, которая позволяет соотнести получаемый уровень доверия со стоимостью и возможностью достижения этой степени доверия. В подходе ISO/IEC 15408 определяются отдельные понятия для доверия к ОО после завершения оценки и по поддержанию доверия во время эксплуатации ОО.

В ISO/IEC 15408 определены семь иерархически упорядоченных оценочных уровней доверия для оценки уровня доверия к ОО. Каждый последующий ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от предыдущего ОУД к последующему достигается заменой какого-либо компонента доверия иерархичным компонентом из того же семейства доверия (т.е. увеличением строгости, области охвата и/или глубины оценки) и добавлением компонентов из других семейств доверия (т.е. добавлением новых требований). Каждый ОУД включает в себя не более одного компонента каждого семейства доверия, при этом учитываются все зависимости каждого компонента доверия.

Реестр доверенного программного обеспечения и продукции электронной промышленности – перечень программного обеспечения и продукции электронной промышленности, соответствующих требованиям информационной безопасности, созданный для целей обеспечения обороны страны и безопасности государства.

Включение в реестр классифицируется по виду и назначению.

Включению в реестр подлежит ПО, являющееся программным продуктом и выполненное в виде самостоятельной программы.

Программные продукты, являющиеся частями ПО, включаются в реестр в составе ПО, частью которого они являются.

Включению в реестр подлежат сервисные программные продукты, созданные в рамках переходных положений, предусмотренных правилами создания, развития, эксплуатации, приобретения объектов информатизации "электронного правительства", а также информационно-коммуникационных услуг, утвержденных уполномоченным органом в сфере информатизации.

Сведения, содержащиеся в реестре, являются открытыми и доступными для ознакомления заинтересованных лиц.

Критериями по включению программного обеспечения в реестр являются:

1) исключительное право на ПО на территории РК или право использования исключительных имущественных прав ПО на территории РК на весь срок действия исключительного права, принадлежащего одному либо нескольким из следующих лиц: физическому/им лицу/ам или юридическому лицу РК;

2) выполнение требований информационной безопасности в соответствии с СТ РК ISO/IEC 15408-3-2017 "Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты" не ниже 4 уровня доверия для ПО или наличие акта по результатам испытаний на соответствие требованиям информационной безопасности (Методика).

Критериями по включению продукции электронной промышленности в реестр являются:

1) исключительное право на объект промышленной собственности или передача права пользования объектом промышленной собственности на весь срок действия, принадлежащего одному либо нескольким из следующих лиц (правообладателей): физическому/им лицу/ам или юридическому лицу РК;

2) соответствие программного обеспечения, входящего в состав продукции электронной промышленности, требованиям информационной безопасности в соответствии с СТ РК ISO/IEC 15408-3 не ниже 4 уровня безопасности (сертификат) или наличие акта испытаний.

Сертификация программного обеспечения на соответствие СТ РК ISO/IEC 15408-3 включает :

* проведение работ по сертификации программного обеспечения (программного продукта) заявителя на соответствие оценочному уровню доверия, согласно заявлению и проверочного листа;
* проведение работ по инструментальному обследованию программного обеспечения (программного продукта) на наличие уязвимостей;
* формирование заключения по результатам проверки.

Порядок проведения испытаний

* отбор образцов и идентификацию образцов;
* составление программы сертификационных испытаний;
* проведение испытаний;
* оценку производства (если это предусмотрено схемой сертификации);
* анализ протоколов испытаний, экспертное заключение.

Рекомендуемая литература

1. Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V.

2. Постановление Правительства РК от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»

3 СТ РК ISO/IEC 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.

4 Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ «Об утверждении методики и правил проведения испытаний объектов информатизации "электронного правительства" и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности».

5 СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования

6 СТ РК ISO/IEC 27002-2015 Информационная технология Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации

Контрольные задания для СРС

1. К объектам информатизации, подлежащим обязательным испытаниям на соответствие требованиям ИБ, относят?

2. Методика проведения испытаний объектов информатизации включает?

3. Проведение испытаний объектов информатизации на соответствие требованиям информационной безопасности регламентируется?

4. Испытания на соответствие требованиям ИБ включают следующие виды работ?

5. Критериями по включению ПО в реестр доверенного ПО и продукции электронной промышленности являются?

6. Составить 5 тестовых заданий различных форм по теме лекции