УТВЕРЖДАЮ
Первый проректор
КарГУ им.академика Е.А.Букетова

_____ Р.М.Жумашев
_____ 2013 г.

Методика обеспечения компьютерной безопасности системы электронного университета

2013

Содержание

1 МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В соответствии с Концепцией информационной безопасности Республики Казахстан, СЭУ ГО, как часть информационной инфраструктуры «электронного правительства», отнесена к классу общегосударственных информационных и коммуникационных систем.

Главной целью, на достижение которой направлены все положения Политики, является надежное обеспечение информационной безопасности Общества и, как следствие, недопущение нанесения материального, физического, морального или иного ущерба Обществу в результате проектно-технологической и информационной деятельности.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование СЭУ;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой на средствах вычислительной техники и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой в СЭУ и передаваемой по каналам связи.

Для достижения поставленной цели необходимо решить следующие задачи:

- защита от вмешательства посторонних лиц в процесс функционирования СЭУ;
- разграничение доступа зарегистрированных пользователей к информации аппаратными, программными и криптографическими средствами защиты, используемыми в СЭУ;
- регистрация действий пользователей при использовании ресурсов СЭУ в системных журналах;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации искажения;
- контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносных кодов, включая компьютерные вирусы;
- обеспечение аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

2 РЕАЛИЗАЦИЯ МЕТОДИКИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Методика обеспечения компьютерной безопасности СЭУ является методологической базой:

- выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;
- обеспечения информационной безопасности;
- координации деятельности структурных подразделений при проведении работ по соблюдению требований обеспечения информационной безопасности.

Для реализации Методики компьютерной безопасности СЭУ необходимо провести комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов, включающих в себя требования в адрес персонала, менеджеров и технических служб. На основе Методики строится управление информационной безопасностью.

Методика сформирована на основе результатов информационного и технического обследования СЭУ в рамках аудита, результатов анализа информационных рисков и оценки защищенности информации, в соответствии с требованиями нормативно-руководящих документов РК, а также согласно рекомендациям международных стандартов в области защиты информации.

Методика основана на системном подходе, гарантирующем высокую вероятность достижения тактической цели - снижения неэффективности разрозненных решений, и стратегической цели - реализации возможностей единого системного решения.

Методика является неотъемлемой частью политики информационной и общей безопасности университета, а в случае отсутствия таковой является основополагающим документом в вопросах обеспечения информационной безопасности СЭУ.

При наличии обеих политик приоритетной является методика обеспечения компьютерной безопасности университета.

Сокращения, термины и определения, используемые в данном документе

В настоящем документе применяются термины и определения в соответствии с СТ РК 34.005-2002 «Информационная технология. Основные термины и определения», ISO/IEC 17799:2005 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью».

В документе также употребляются следующие определения, понятия и

соглашения, наиболее часто используемые в среде информационной безопасности:

администратор безопасности информационных систем - работник, обеспечивающий исполнение мер по информационной безопасности;

атака – несанкционированная деятельность с вредоносными намерениями, использующая специально разработанный программный код или специальные методики;

аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа реализованными в системе;

авторизация – определение по данным аутентификации полномочий лица или информационного ресурса и элементов, к которым им следует предоставить доступ;

база данных (БД) - упорядоченная совокупность данных и структур их хранения, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, и предназначенная для обработки с помощью средств вычислительной техники;

вероятность реализации угрозы через данную уязвимость - степень возможности реализации угрозы через данную уязвимость в тех или иных условиях;

вредоносное программное обеспечение – программное обеспечение создаваемое с целью причинения вреда информационным системам и информационным ресурсам;

защита информации - принятие правовых, организационных и технических (программно-технических) мер в целях обеспечения целостности сохранности информации, недопущения ее несанкционированного изменения или уничтожения, соблюдения конфиденциальности информации ограниченного доступа, реализации права на доступ к информации, а также недопущения несанкционированного воздействия на средства обработки, передачи и хранения информации;

защита информации от несанкционированного доступа - меры, направленные на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными правовыми актами или собственником, владельцем информации прав или правил доступа к ней;

защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиям, устанавливаемыми собственником информации, которыми может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо;

защита программных средств - организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и

устранение последствий этих действий;
идентификатор - уникальный персональный код, присвоенный субъекту и объекту системы, предназначенный для регламентированного доступа к системе и ресурсам системы;
идентификация - определение соответствия предъявленного для получения доступа в систему, к ресурсу идентификатора перечню идентификаторов, имеющихся в системе;
несанкционированный доступ к информации – получение защищаемой информации, заинтересованным субъектом, с нарушением установленных правовыми документами правил доступа к ней;
несанкционированный доступ к программным средствам - доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил;
пользователь - человек, организация, система, использующие в своей работе в той или иной мере компьютер, вычислительную систему, базу данных, сеть и пр. Очень широкое понятие, которое может заменять понятия: оператор, программист, абонент и т.д.;
доступ - перемещение людей, транспорта и других объектов в (из) помещения, здания, зоны и территории;
разграничение доступа - порядок доступа лиц к техническим и программным средствам, защищаемой информации при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами*;*
рабочее место – оборудованное *рабо́чее ме́сто пользователя (администратора)* — стол, стул, компьютер, с установленными необходимыми ПО, в том числе СЭУ и подключенный к телекоммуникациям;
рабочая станция – комплекс технических и программных средств предназначенных для решения определенного круга задач;
система обеспечения информационной безопасности – система мер направленная на выявление угроз информационной безопасности, предотвращения и пресечения их реализации, а также ликвидации последствий реализованных в результате НСД;
средства вычислительной техники – совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем;
средства защиты информации – технические, криптографические, программные и другие средства, вещества или материалы, предназначенные или используемые для защиты информации;
средства криптографической защиты информации – средства, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности;
средства обеспечения информационной безопасности – совокупность

правовых, организационных, и технических мероприятий, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба любого характера собственнику и потребителю информации;
технический канал утечки информации – совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об объекте, и физической среды, в которой распространяется информационный сигнал;
техническое обеспечение – комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы;
угроза доступности – угроза нарушения работоспособности информационной системы при доступе к информации;
угроза конфиденциальности – угроза раскрытия информации;
угроза целостности – угроза изменения информации;
угрозы информационной безопасности – совокупность причин, условий и факторов, создающих опасность для объектов информационной безопасности, реализация которых может повлечь нарушение прав, свобод и законных интересов юридических и физических лиц в информационных процессах;
утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками;
ISO – Международная организация по стандартизации (International Organization for Standardization, ISO), занимающаяся выпуском стандартов;
IEC – Международная электротехническая комиссия (МЭК; англ. International Electrotechnical Commission, IEC) — международная организация по стандартизации в области электрических, электронных и смежных технологий;

Используемые сокращения.

В настоящем документе использованы следующие обозначения и сокращения:

СЭУ	Система электронного университета
ИБ	Информационная безопасность
ИС	Информационная система
ИЗ	Информационная защита
НПА	Нормативно-правовой акт
НСД	Несанкционированный доступ
ПО	Программное обеспечение
РК	Республика Казахстан
СЗИ	Система защиты информации
ЭЦП	Электронная цифровая подпись

3 ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА СЭУ

3.1 Область применения Политики информационной безопасности СЭД КарГУ

Область и границы применения настоящего документа охватывают:

САПИ – система авторизации пользователей университета для доступа к интернету

СЭД – систему электронного документооборота

ТЕСТЕР – система организации тестирования

СЭУ спроектирована с использованием принципа «ролевого распределения функций» между пользователями и обслуживающим персоналом. Выполнение ролевых функций конкретным должностным лицом в университете определяется его руководством.

Перечень ролей, входящих в область действия ПИБ и состава их функциональных обязанностей, приведен в Таблица 1.

Таблица 1

№	Наименование роли	Описание функциональных обязанностей роли
1	Администратор	Выполнение настройки различных параметров системы. Управление правами доступа к функциям и объектам системы. Мониторинг работы пользователей и системы в целом.
2	Студент	Доступ к тестовым вопросам во время сессии; Просмотр личной информации
3	Сотрудник	Определение хода исполнения документов в форме резолюций, в которых содержатся поручения к исполнению Подписание документов организации
4	Преподаватель	Загрузка тестовых вопросов в базу данных в соответствии с графиком
5	Ответственное лицо	Доступ к информации решаемой задачи

Функции подсистемы СЭД

- контроль передачи основных реквизитов документа;
- учет хранящихся документов в процессе делопроизводства;
- генерация сообщений о событиях в системе;
- обработка документов (документооборот);
- учет документов в процессе делопроизводства;
- маршрутизация документов на всех уровнях его обработки (доставка пользователям);
- контроль исполнения документов;
- учет и архивное хранение документов;
- обмен документами между территориальными подразделениями университета;
- поддержка нормативно-справочной информации системы;
- актуализация содержания полей документов при изменении справочной информации (перевод сотрудника из одного структурного подразделения университета в другое, увольнение сотрудника);
- управление правами доступа к объектам системы;

4 МЕТОДОЛОГИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ

Целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в ресурсы СЭУ.

В общем контексте безопасность связана с защитой ресурсов от угроз, где угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами.

При разработке политики безопасности использована модель (рис.1) соответствующая международному стандарту ISO/IEC 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью».

Источники угроз – это силы природы, объекты окружающей среды, деструктивные социальные проявления и т. п., которые могут нанести хаотический ущерб ресурсам при возникновении, активизации или изменении своего состояния без стремления к достижению какой-либо цели.

Нарушители – это субъекты и объекты посредством субъектов, которые нанесли ущерб в результате неформализованных действий или бездействия без стремления к достижению какой-либо заранее спланированной цели.

Ресурсы - это данные, создаваемые в процессе функционирования и эксплуатации ПО СЭУ, а также программно-аппаратное обеспечение входящие в эксплуатационный комплект СЭУ.

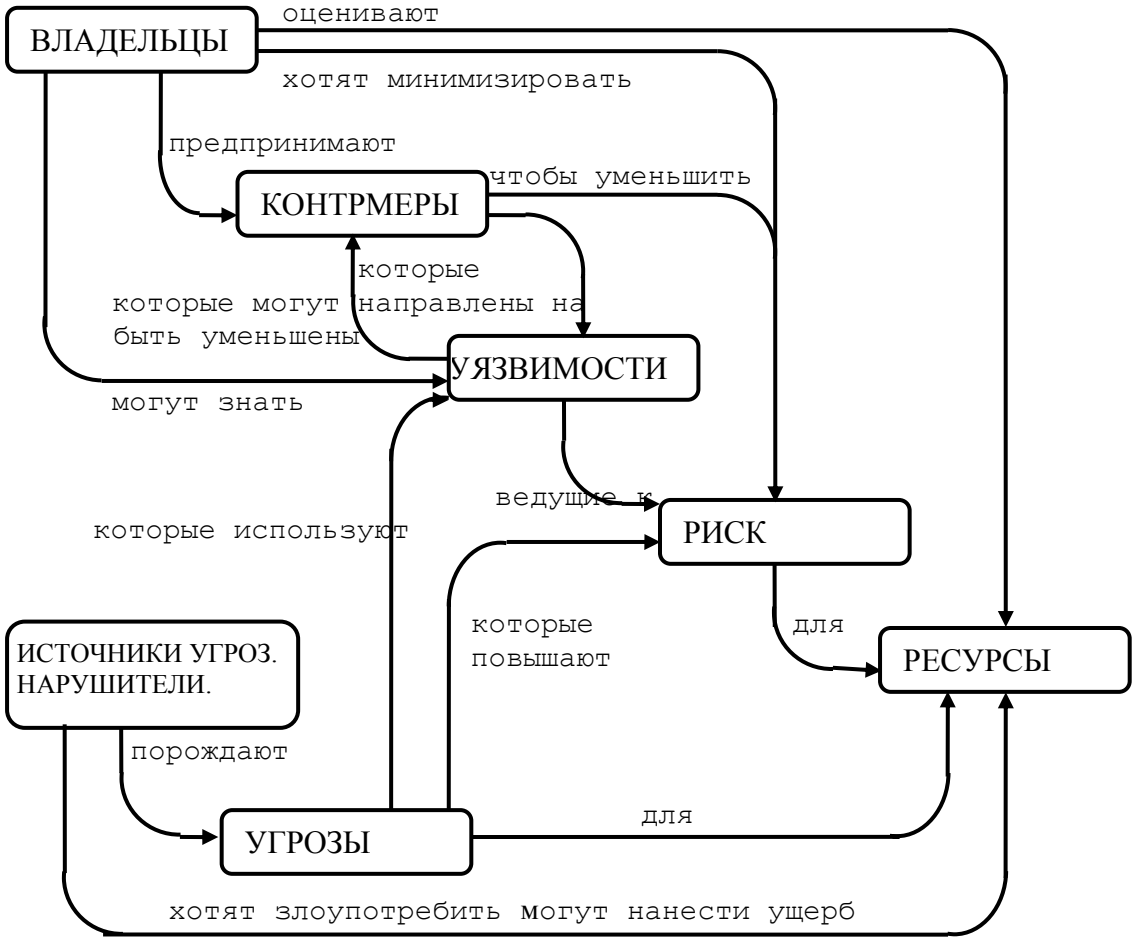

Рисунок 1 – Модель безопасности

Контрмеры – предупреждающие действия (решения) принимаемые ГО для предотвращения уязвимости.

Риски - сочетание вероятности наступления уязвимости и его последствий для ресурсов СЭУ.

Уязвимость – это потенциальные опасности для функционирования СЭУ. В общем случае, уязвимость ассоциируется с нарушением политики безопасности, вызванным неправильно заданным набором правил или ошибкой в обеспечивающей безопасность компьютера программе.

Уязвимость — это состояние системы, которое позволяет:

- исполнять команды от имени другого пользователя;
- получать доступ к информации, закрытой от доступа для данного пользователя;
- показывать себя как иного пользователя или ресурс;

Отдельные категории нарушителей могут быть отнесены к разряду злоумышленников, определяемых как «лицо, которое совершает, или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть

возможность наступления этих последствий». Поскольку такое определение применяется к нарушителю только по решению суда, по понятным причинам далее применяется термин «нарушитель».

Потенциальные нарушители - это субъекты и объекты посредством субъектов, которые могут нанести ущерб в определенных условиях при наступлении определенных событий.

За сохранность рассматриваемых ресурсов отвечают их владельцы (в контексте документа организация, эксплуатирующая СЭУ), для которых эти ресурсы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим ресурсам и стремиться использовать их вопреки интересам их владельца.

Владельцы воспринимают подобные угрозы как потенциал воздействия на ресурсы, приводящего к понижению их ценности для владельца. К специфическим нарушениям безопасности обычно относят (но не обязательно ими ограничиваются): раскрытие ресурса несанкционированным получателем, наносящее ущерб (потеря конфиденциальности); ущерб ресурсу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к ресурсу (потеря доступности).

Владельцы ресурсов анализируют возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ помогает при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Таким образом, ПИБ основывается на модели, которая рассматривает три основных субъекта — владельца, службу информационной безопасности собственника, нарушителя. Владелец передает процессы обеспечения безопасности службе ИБ.

Изначально у службы ИБ отсутствуют знания о нарушителе.

Для построения модели нарушителя в этих условиях используется принцип «черного ящика», действующего как генератор событий, направленных на активизацию угроз через уязвимости, что является достаточным для обеспечения базового уровня безопасности.

В основу разработки и практической реализации методики обеспечения компьютерной безопасности положены следующие принципы:

1) Невозможность миновать защитные средства;
2) Усиление самого слабого звена;
3) Недопустимость перехода в открытое состояние;
4) Минимизация привилегий;
5) Разделение обязанностей;
6) Многоуровневая защита;
7) Разнообразие защитных средств;
8) Простота и управляемость информационной системы;
9) Обеспечение всеобщей поддержки мер безопасности.

Принцип невозможности миновать защитные средства означает, что все

информационные потоки в подсистемы СЭУ и из них должны проходить через СЗИ.

Надежность любой СЗИ определяется самым слабым звеном. Часто таким звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип недопустимости перехода в открытое состояние означает, что при любых обстоятельствах (в том числе и нештатных), СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно для предотвращения злонамеренных или неквалифицированных действий системного администратора.

Принцип многоуровневой защиты предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — управление доступом и, как последний рубеж, — протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления СЗИ.

Принцип простоты и управляемости информационной системы в целом и СЗИ в особенности определяет возможность формального или неформального доказательства корректности реализации механизмов защиты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Рекомендуется с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

5 УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЭУ, МЕТОДЫ И СРЕДСТВА

В разделе 4 Концепции информационной безопасности Республики Казахстан, далее по тексту раздела - Концепции, положениями которой, согласно Указу Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан» №199 от 10 октября 2006 года, надлежит руководствоваться в своей деятельности государственным органам и организациям, определены основные угрозы информационной безопасности, их виды, направления и возможные источники исхода/возникновения.

5.1.Виды угроз

Основными действиями, которые производятся с информацией и могут содержать в себе угрозу, являются сбор, модификация, утечка и уничтожение данных. Эти действия являются базовыми для дальнейшего рассмотрения.

В Концепции определены основные виды угроз информационной безопасности, порождающие их действия, их источники.

Практически все они в явном или неявном виде присутствуют в СЭУ и могут быть представлены следующим образом.

Придерживаясь принятой в Концепции классификации, все источники угроз СЭУ разделяются на внешние и внутренние.

Источниками внутренних угроз являются:

1. сотрудники организации;
2. ПО;
3. аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

1. ошибки пользователей и системных администраторов;
2. нарушения сотрудниками установленных регламентов сбора, обработки, передачи и уничтожения информации;
3. ошибки в работе ПО;
4. отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

1. компьютерные вирусы и вредоносные программы;
2. организации, службы и отдельные лица;
3. стихийные бедствия.

Формами проявления внешних угроз являются:

1. заражение компьютеров вирусами или вредоносными программами;
2. несанкционированный доступ (НСД) к корпоративной информации;
3. информационный мониторинг со стороны конкурирующих структур;
4. аварии, пожары, техногенные катастрофы.

5.2 Методы и средства информационной безопасности СЭУ

Обеспечение информационной безопасности СЭУ реализуется следующими формами защиты:

1. правовой;
2. организационной;
3. программно- аппаратной.

5.2.1 Правовые методы обеспечения информационной безопасности СЭУ

Основой правовой формы обеспечения информационной безопасности СЭУ являются:

- Закон Республики Казахстан от 7 января 2003 года №370- II «Об электронном документе и электронной цифровой подписи» (с изменениями, внесенными Законом РК от 20.12.04 г. №13- III);
- Закон Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации»;
- Закон Республики Казахстан от 12 января 2007 года № 221-III «О порядке рассмотрения обращений физических и юридических лиц»;
- Указ Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан» №199 от 10 октября 2006 года;
- Постановление Правительства Республики Казахстан от 17 апреля 2004 года N 430 «Об утверждении Правил электронного документооборота государственных органов Республики Казахстан»;
- Постановление Правительства Республики Казахстан от 22 января 2003 года N 77 «Об утверждении перечня продукции, соответствие которой допускается подтверждать декларацией о соответствии»;
- Постановление Правительства Республики Казахстан от 29 ноября 2000 года N1787 «О контроле соответствия продукции в Республике Казахстан» (с изменениями, внесенными постановлениями Правительства РК от 05.04.02 г. N 407; от 08.08.02 г. N 888; от 28.07.03 г. N 751);
- Постановление Правительства Республики Казахстан от 14 сентября 2004 года N 965 «О некоторых мерах по обеспечению информационной безопасности в Республике Казахстан»;
- Правила регистрации, выдачи, хранения, отзыва (аннулирования) регистрационных свидетельств Утвержденные Приказом Председателя Агентства Республики Казахстан по информатизации и связи от 07 декабря 2005г. № 457-п;
- Типовое положение удостоверяющего центра Утверждено Приказом Председателя Агентства Республики Казахстан по информатизации и связи от 08 декабря 2005г. № 458-п;
- Положение о закреплении и разграничений функций и полномочий администраторов системы «название системы»;
- Инструкция о порядке действий пользователей во внештатных (кризисных) ситуациях в системе «название системы»;

- Регламент резервного копирования информации;
- Правила регистрации пользователей в системе «название системы»;
- Регламент доступа пользователей и администраторов к серверам.

5.2.2 Организационные формы защиты

Организационной формой защиты являются (но не ограничиваются) мероприятия, предусмотренные данной методикой. К ним относятся:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании технической инфраструктуры СЭУ и других ассоциированных с ней объектов;
- мероприятия по разработке правил доступа пользователей к ресурсам системы согласно политике безопасности;
- мероприятия, осуществляемые при подборе и подготовке персонала, сопричастного с СЭУ;
- организацию охраны и режима допуска к системе;
- организацию учета, хранения, использования и уничтожения документов и носителей информации;
- распределение реквизитов разграничения доступа;
- организацию контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и ПО.

Физическая безопасность

Критическое или чувствительное оборудование обработки информации должно быть размещено в охраняемых зонах, защищено определенными периметрами безопасности, оснащенными соответствующими барьерами безопасности и средствами контроля на входе. Они должны быть физически защищены от несанкционированного доступа, повреждения или создания помех в работе.

Применительно к *безопасности окружающей среды* должны быть разработаны (и применяться) меры по физической защите от ущерба в результате пожаров, наводнений, землетрясений, взрывов, массового гражданского неповиновения, а также от других видов бедствий естественного или искусственного характера. Такие меры содержатся в действующих в организации правилах, инструкциях и иных документах по пожарной безопасности, электробезопасности, действиях в условиях чрезвычайных ситуаций.

Обеспечиваемая защищенность должна быть пропорциональна идентифицированным рискам.

Физическая безопасность реализуется совокупностью способов защиты на основе инженерных конструкций в сочетании с техническими средствами охраны, образующих физическую защиту. Составной частью физической

защиты - является инженерная защита и техническая охрана объектов (ИЗТОО).

Требуемый уровень информационной безопасности достигается многозональностью и многорубежностью защиты, которая должна быть обеспечена с помощью инженерной защиты и охраны системы СЭУ.

Организационно – технологическая среда СЭУ представляет собой единый комплекс информационных и технических ресурсов, эксплуатирующего и обслуживающего персонала.

Технические ресурсы СЭУ в целом не являются внутренним изолированным объектом, использующимся исключительно для ее нужд.

Они топологически наложены на техническую инфраструктуру университета:

1. на рабочих станциях пользователей СЭУ-В решается целый комплекс других задач, не имеющих отношения к системе СЭУ;
2. общие инженерные сети, здания, помещения, комнаты, сейфы…

Применительно к вопросам физической безопасности СЭУ. К предметами рассмотрения являются:

- Рабочее место пользователя
- Сервер (одно или несколько логически объединенных устройств)
- Серверное помещение
- Рабочее место администратора СЭУ
- Съемные носители информации
- Средство хранения резервных носителей

Требования к рабочему месту пользователя (администратора) СЭУ

В состав типового рабочего места пользователя СЭУ-В входят:

1) компьютер (комплект – системный блок, монитор, клавиатура, манипулятор «мышь», многогнездная розетка-удлинитель (опция), источник бесперебойного питания (опция));

2) мебель рабочего места (стол письменный (канцелярский), стул, тумбочка).

В целях обеспечения требований физической безопасности компьютер как комплект должен быть проверен на информационную безопасность по уровню излучения/воздействия побочных электромагнитных излучений и наводок (ПЭМИН) и соответствующим образом сертифицирован и опломбирован. В случае обнаружения факта, изменения состава комплекта или нарушения пломбы сертификат считается отозванным, дальнейшее использование компьютера прекращается и может быть возобновлено только по результатам сертификации или заключения экспертной комиссии.

Категорически запрещается совместное использование с компьютером внешних устройств с беспроводным подключением (клавиатура, мышь).

Категорически запрещается использование переносных розеток-удлинителей низкого качества, изготовленных полукустарным способом, и

могущих стать источником возгорания или поражения персонала электрическим током.

Должно быть минимизировано количество путей доступа к ресурсам компьютера, удалить (физически отключить) «лишние», неиспользуемые для повседневной штатной работы порты (COM, USB, RS,…), флоппи и CD/DVD дисководы.

Монитор следует располагать таким образом, чтобы исключить возможность просмотра содержимого экрана посторонними лицами, в том числе извне с помощью оптических приборов.

Порядок и условия хранения носителей с ключами ЭЦП и средств криптографической защиты информации регламентированы Правилами регистрации, выдачи, хранения, отзыва (аннулирования) регистрационных свидетельств, в том числе их копий на бумажном носителе и ведения регистра регистрационных свидетельств.

Не следует загромождать поверхность рабочего стола не используемыми в данный момент документами, носителями, а также оставлять их на столе при уходе с рабочего места на продолжительное (например, более 2 часов) время. Следует соблюдать режим «чистого стола» - ничего лишнего, только самое необходимое на данный момент работы.

Аналогичные правила должны распространяться и на «рабочий стол» монитора. Не следует держать открытыми большое число «окон» или сбрасывать их в строку состояния. Должен использоваться паролируемый хранитель экрана.

В качестве носителей информации должны использоваться носители, полученные пользователем непосредственно в организации. Каждый носитель должен иметь заводской номер изготовителя, маркерную метку или не снимаемую этикетку с маркерной меткой организации, датой ввода в эксплуатацию и инвентарным номером ресурса в системе ИБ, соответствующему номеру в карточке ресурса. Использование носителей, не отвечающих этим требованиям, категорически запрещается.

Для хранения носителей с оперативными резервными копиями данных и состояния системы должны быть определены место и средства хранения и соблюдены условия хранения применительно к типу конкретного носителя.

Поскольку состав рабочего места администраторов в целом соответствует вышеприведенному, аналогичные требования и рекомендации распространяются также и на рабочие места администраторов.

Требования к серверному оборудованию и серверному помещению

Требования к серверу как к единице оборудования в отношении ИБ в целом соответствуют требованиям, предъявляемым оборудованию системы.
Общие требования к серверному помещению должны отвечать требованиям, приведенным в технической документации изготовителя или стандарте EIA/TIA 569.

Стойка (шкаф) сервера должны быть закрыты со всех сторон стенками и запираться на ключ (если это предусмотрено конструкцией). Не должно быть понятий «зимнего» и «летнего» режима, когда сервер эксплуатируется со снятыми стенками.

В зависимости от конструктивных особенностей, сервер может поставляться как в виде комплектного моноустройства, так и в виде отдельных блоков, предназначенных для монтажа в аппаратную стойку или шкаф, в том числе и открытого исполнения, что приводит к ликвидации одного рубежа защиты, поскольку невозможно устранить неконтролируемый физический доступ к элементам сервера, также существенно усложняется и сертификация. В этом случае ужесточаются требования к серверному помещению в части контроля доступа, которые должны компенсировать ликвидацию одного рубежа защиты. Должны быть обязательно предусмотрены: металлическая дверь с замком повышенной секретности, система контроля доступа с выводом сигнала тревоги на ПЦО, система видеонаблюдения. Физический доступ персонала в серверное помещение должен осуществляться согласно указаниям п. 9.1.2 стандарта ISO 17799.

Особое внимание следует уделять физическому порядку в серверном помещении. Категорически запрещается использовать серверное помещение для складирования посторонних предметов. Необходимо составить перечень оборудования из состава сервера и задействованных обеспечивающих систем (UPS, автономный кондиционер и т.д.), нахождение которого обоснованно необходимо в серверном помещении, указать ответственного за поддержание порядка. Перечень в распечатанном виде должен быть помещен на видное место.

В целях обеспечения работоспособности, возможности производительной эксплуатации в течение всего срока службы оборудования необходимо выполнять комплекс ремонтно-профилактических мероприятий, предусмотренный технической документацией. С этой целью составляется план таких работ в рамках внутри- и межремонтных циклов с указанием вида, даты начала и планируемого окончания работ.

При производстве всех видов ремонтно-профилактических работ должны быть предусмотрены меры по недопущению реализации угрозы типа «отказ в доступе». С этой целью рекомендуется до начала выполнения работ предусмотреть возможность перехода на резервный режим и проверить готовность такого перехода.

5.2.3 Программные и аппаратные формы защиты

Программными и аппаратными формами защиты являются (но не ограничиваются) мероприятия, предусмотренные данной ПИБ. К ним относятся:

а) идентификацию и аутентификацию пользователей;

b) разграничение доступа к ресурсам;
c) регистрацию событий;
d) криптографические преобразования;
e) проверку целостности системы;
f) проверку отсутствия вредоносных программ;
g) программную защиту передаваемой информации и каналов связи;
h) защиту системы от наличия и появления нежелательной информации;
i) создание физических препятствий на путях проникновения нарушителей;
j) мониторинг и сигнализацию соблюдения правильности работы системы;
k) создание резервных копий информации.

Защита электронного обмена данными

Информация, передаваемая в виде электронных сообщений, должна быть соответствующим образом защищена. Для обмена данными и обеспечения коммуникационного потока в СЭУ используется СГДС, свойства которой позволяют обеспечить требуемый уровень ИБ. Однако ИБ СЭУ в целом зависит и от состояния ИБ при обмене сообщениями в других системах, функционирующих на тех же технических средствах, что и СЭУ. При рассмотрении безопасности электронного обмена данными в этих системах необходимо учитывать следующее:

a) должна быть предусмотрена защита сообщений от несанкционированного доступа, изменения или отказа в обслуживании;
b) должна быть обеспечена правильная адресация и транспортировка сообщения;
c) должна быть обеспечена надежность и доступность обслуживания;
d) должны быть учтены требования законодательства, в частности, требования, предъявляемые к ЭД и ЭЦП;
e) должно быть предусмотрено использование более строгих правил идентификации при доступе из сетей общего пользования и обеспечен контроль их соблюдения.

Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием электронной почты, следует применять (по необходимости) соответствующие средства контроля. Необходимо учитывать:

a) уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

b) уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например, неправильная адресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;
c) влияние изменения характеристик коммуникационной среды на производственные процессы, например, влияние повышенной скорости передачи данных или изменения системы адресации между организациями и отдельными лицами;
d) правовые соображения, такие, как необходимость проверки источника сообщений и др.;
e) последствия для системы безопасности от раскрытия содержания каталогов;
f) необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

Организации должны задать четкие правила, касающиеся статуса и использования электронной почты.

6 ПЕРЕЧЕНЬ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ, НА ОСНОВЕ КОТОРЫХ РАЗРАБОТАНА МЕТОДИКА

1. Закон Республики Казахстан от 11.01.2007 №217 – III «Об информатизации».

2. Закон Республики Казахстан от 15 марта 1999 года № 349-I «О государственных секретах» (с изменениями и дополнениями по состоянию на 02.04.04 г.).

3. Закон Республики Казахстан от 26 июня 1998 года № 233-I «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 14.10.2005 г.).

4. Указ Президента Республики Казахстан от 14 марта 2000 г. N 359 «О Государственной программе обеспечения информационной безопасности Республики Казахстан на 2000-2003 годы».

5. Концепция информационной безопасности Республики Казахстан». Одобрена Указом Президента Республики Казахстан от 10 октября 2006 года, № 199.

6. Международный стандарт ISO/IEC FDIS 17799:2005. Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью.

7. СТ РК 34.005-2002. Информационная технология. Основные термины и определения

Приложение 1

Правила регистрации пользователей СЭУ

1. Общие положения

1. Настоящие «Правила регистрации пользователей» (далее - Правила) устанавливают единый порядок регистрации пользователей при предоставлении (изменении уровня, удалении) доступа к единой системе электронного документооборота (далее – ИС) как производственному средству для выполнения ими работ в пределах своих должностных обязанностей (роли).

2. Регистрация пользователей проводится с целью установления информационных границ области производственной деятельности каждого пользователя ИС и обеспечения принципа персональной ответственности каждого пользователя за свои действия. Целью настоящих правил является также обеспечение ИБ на уровне контроля доступа и аутентификации.

В качестве пользователей ИС могут быть зарегистрированы только штатные сотрудники организации по представлению руководства подразделения.

2. Порядок регистрации

1. Для получения доступа к информационным ресурсам ИС пользователь заполняет заявку на регистрацию (далее – Заявка) по форме [ФЗ -1], приведенной в приложении.
2. Заявка с указанием необходимого уровня доступа подается на имя лица, курирующего подразделение, ответственное за ИС. Уровень доступа к ресурсам ИС определяет руководитель подразделения пользователя по согласованию с подразделением, ответственным за информационную безопасность.
3. Пользователь, после полного согласования с причастными структурными подразделениями, указанными в заявке, передает заявку в подразделение, ответственное за ИС.
4. Администраторы ИС регистрируют пользователя в ИС с предоставлением ему доступа к информационным ресурсам согласно удовлетворенной Заявке.
5. Подразделение, ответственное за ИС, отвечает за своевременное предоставление доступа к ресурсам ИС, правильное заполнение всех позиций Заявки на регистрацию, своевременное удаление аннулированной учетной записи из списка пользователей.
6. По решению руководства, а также по представлению службы ИБ заявка может быть отклонена или аннулирована.

3. Требования к элементам регистрации

1. Для работы в ИС пользователю необходимо иметь имя и пароль, получаемые им в процессе регистрации
2. Результатом выполнения процесса регистрации является формирование в составе БД ИС учетной записи пользователя.
3. В качестве пароле используется случайная последовательность символов. Пароль должен отвечать следующим требованиям:
4. Длина пароля должна быть не менее 8 символов;
5. В числе символов пароля обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (§, @, #, $, &, *, % и тому подобное);
6. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименование автоматизированного рабочего места - АРМ и так далее), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
7. Пароль может использоваться на протяжении максимум 12 месяцев. При использовании доменной учетной записи, срок действия пароля не более 30 дней. По истечении этого периода система должна потребовать от пользователя изменить его. Данное требование в принудительном порядке реализуется посредством программного обеспечения аутентификации;

4. Уровни доступа к ИС, роли и порядок их назначения

В целях обеспечения информационной безопасности ИС, а также определения зоны ответственности и компетентности каждого пользователя ИС используется процедура назначения и поддержки уровней доступа и ролей. Ответственность за выбор пары «уровень доступа – роль» несет руководитель подразделения пользователя.

При назначении уровня доступа и ролей, указанным в заявке, администратор обязан осуществлять контроль их совместимости и непротиворечивости: доступ к объектам и перечень разрешенных действий над ними на уровне доступа и права роли должны быть приведены к взаимному соответствию.

5. Права и обязанности пользователя ИС

1. Пользователь при выполнении своих обязанностей имеет право использовать ресурсы ИС в полном объеме в соответствие с установленными уровнем доступа и правами.
2. Пользователь не имеет права работать под чужими логином и/или паролем. В случае, если руководство предлагает пользователю работать в таких условиях, пользователь вправе потребовать письменного

указания (приказа) руководства, согласованного со службой ИБ, и не приступать к работе до получения такого указания (приказа).

3. Пользовать имеет право проверять содержание своей учетной записи.
4. Пользователь обязан обеспечить конфиденциальность и сохранность логина и пароля. При компрометации своих регистрационных данных пользователь должен незамедлительно оповестить об этом непосредственного руководителя (сотрудника ИБ, администратора ИС).
5. Пользователь обязан сообщать обо всех ставших ему известными фактах компрометации паролей других сотрудников в службу ИБ.
6. При увольнении из организации, переходе в другое подразделение или любом другом событии, при котором изменилась вышеуказанная информация, пользователь (руководитель пользователя) обязан сообщить об этом администратору ИС.
7. Для удаления/изменения своей учетной записи пользователь обязан подать Заявку по форме ФЗ-1, администратор на основании этой заявки ИС обязан уничтожить/изменить учетную запись пользователя в системе, внести соответствующую запись в журнал регистрации пользователей и сообщить об этом подразделению, ответственному за информационную безопасность.

6. Корпоративная этика

Особый психологический настрой и моральные стимулы программисту может создать особые корпоративные условия его деятельности, в частности различные моральные обязательства, оформленные в виде кодексов чести. Ниже приводится "Кодекс чести пользователя компьютера".

- Обещаю не использовать компьютер в ущерб другим людям.
- Обещаю не вмешиваться в работу компьютера других людей.
- Обещаю "не совать нос" в компьютерные файлы других людей.
- Обещаю не использовать компьютер для воровства.
- Обещаю не использовать компьютер для лжесвидетельства.
- Обещаю не копировать и не использовать чужие программы, которые были оплачены не мною.
- Обещаю не использовать компьютерные ресурсы других людей без разрешения и соответствующей компенсации.
- Обещаю не присваивать результаты интеллектуального труда других людей.
- Обещаю думать об общественных последствиях разрабатываемых мною программ или систем.
- Обещаю всегда использовать компьютер с наибольшей пользой для живущих ныне и будущих поколений.