КЛАССИФИКАЦИЯ И ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

CLASSIFICATION AND MAJOR THREATS TO INFORMATION SECURITY

Абдикаликов К.А.

Актюбинский государственный университет им. К.Жубанова, г.Актобе, Казахстан,

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности. Национальная безопасность государства существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре.

Информационная безопасность является одной из составляющих национальной безопасности республики и оказывает влияние на защищенность национальных интересов в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Республики Казахстан и методы ее обеспечения являются общими для этих сфер.

Наряду с интенсивным развитием вычислительных средств и систем информации все более актуальной становится проблема обеспечения ее безопасности. Прежде чем провести анализ угроз информационной безопасности, определим основные понятия и классифицируем виды и типы существующих угроз информационной безопасности

Под угрозой безопасности информации понимается действие, которое может привести прямо или косвенно к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства. Угрозы безопасности обычно принято делить на случайные и умышленные.

По целям реализации угрозы;

По принципу воздействия на ИВС;

Под доступом понимается взаимодействие между субъектом и объектом, приводящее к возникновению информационного потока от второго к первому.

Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким способом, который нарушает системную политику безопасности.

По характеру воздействия различают *активное* и *пассивное* воздействие.

Активное угрозы имеют целью нарушение нормального процесса функционирования посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы.

Пассивное угрозы направлены на несанкционированное использование информационных ресурсов, не оказывая при этом каких-либо побочных эффектов и в их анализе.

К основным угрозам безопасности информации относят [1,2,3]:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование информационных ресурсов;

- несанкционированный обмен информацией; отказ от информации;

- отказ в обслуживании.

Наиболее распространенными путями несанкционированный доступ (НСД) к информации, сформулированными на основе анализа зарубежной печати, являются:

Атаки *«салями».* Это атаки более всего характерны для систем, обрабатывающих денежных средства.

«Скрытые каналы». Это передачи информации между процессами системы, нарушающие системную политику безопасности.

«Маскарад». Под «маскарадом» понимается выполнение каких-либо действий одним пользователем АСОИ от имени другого пользователя.

«Сборка мусора». После окончания работы обрабатываемая информация не всегда удаляется из памяти компьютера, хотя при искажении заголовка файла их прочитать трудно, однако, используя специальные программы и оборудование, все же возможно.

«Вредоносные программы». Под вредоносными программами будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

«Тронский конь» - программа, выполняющая в дополнение к основным дополнительные, но не описанные в документации действия.

«Червь» - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе.

«Жадные программы» - программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его.

«Захватчики паролей» - программы, специально предназначенные для перехвата паролей. Для предотвращения этой угрозы, перед входом в систему необходимо убедиться, что вы вводите имя и пароль именно системной программе входа, а не какой-то другой. Постоянно проверяйте сообщения о дате и времени последнего входа и количестве ошибочных входов. Не записывайте команды, содержащие пароль, в командные процедуры, старайтесь избегать явного объявления пароля при запросе доступа по сети, это процесс можно отследить и захватить пароль. Не используйте один и тот же пароль для доступа к разным узлам.

Одними из основных направлений по принятию мер обеспечения информационной безопасности являются:

– *развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;*

– *защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем и сетей, как существующих, так и создаваемых.*

Для достижения этого необходимо:

– *развивать и совершенствовать инфраструктуру единого информационного пространства Республики Казахстан;*

– *развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;*

– *развивать производство конкурентоспособных средств и систем информатизации, телекоммуникации и связи, участвовать в международной кооперации производителей этих средств и систем;*

– *обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.*

СПИСОК ЛИТЕРАТУРЫ

1. Кивиристи А. Новые грани обнаружения и отражения угроз //Системы безопасности – 2000-ноябрь-декабрь – С.44-47.

2. Симонов С.В. Анализ рисков в информационных системах. Практические аспекты //Конфидент – 2001 – №1 – С.48-53.

3. Абдикаликов К.А., Задирака В.К. Элементы современной криптологии и методы защиты банковской информации. – Алматы: Гылым, 1999. – 364с.

СОВРЕМЕННОЕ ТРЕБОВАНИЕ К ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ВУЗЕ

THE CURRENT REQUIREMENT FOR THE TRAINING OF SPECIALISTS IN HIGHER EDUCATION

Кагазбаева А.К.

Актюбинский государственный университет им.К.Жубанова, г.Актобе, Казахстан.

В настоящее время изменения, происходящие в общественной и социальной жизни, ставят перед системой образования принципиально новых задач, качественное решения которых требует преобрзовании систем образования, в том числе системы высшего профессионального образования. Сутью преобразования является повышения качества профессиональной подготовки специалистов путем смены методологии образовательного стандарта. При этом в качестве новой методологии ученые предлагают так называемый «компетентностный» подход к образованию. Основными понятиями данного подхода являются понятия “компетенция” и «ключевая компетенция», «компетентность».

Под компетенцией понимают круг вопросов, в которых личность обладает познанием и опытом, что позволяет ей быть успешной в собственной жизнедеятельности. Сущностным признаком компетенции является постоянная изменчивость, связанная с изменениями к успешности взрослого в постоянно меняющемся обществе. Компетенция проявляется в умении осуществлять выбор, исходя из адекватной оценки своих возможностей в конкретной ситуации, и связанна с мотивацией на непрерывное образование.

Составляющими элементами понятия "компетенция" являются: знания, навыки, способность, усилия.

Компетенции по видам можно делить на ключевые, базовые и функциональные.

Ключевые компетенции – это компетенции, необходимые для жизнедеятельности человека и связанные с его успехом в профессиональной деятельности в быстроизменяющемся обществе, иначе говоря, ключевыми компетенциями можно назвать такие, которыми должен обладать каждый член общества и которые можно было бы применять в самых различных ситуациях. Ключевые компетенции становятся универсальными и применимыми в разных ситуациях.

Под базовыми компетенциями понимаются компетенции, отражающие специфику определенной профессиональной деятельности. Функциональные компетенции представляют собой совокупность характеристик конкретной деятельности и отражают набор функций, характерных для данного рабочего места.

Таким образом, компетенция включает совокупность взаимосвязанных качеств личности, задаваемых по отношению к определенному кругу предметов и процессов. А компетентность соотносится с владением, обладанием человеком соответствующей компетенцией, включающей его личное отношение к ней и предмету деятельности.

В целом, компетентностный подход в образовании предполагает четкую ориентацию на будущее, каторая проявляется в возможности построения своего образования с учетом успешности в личностной и профессиональной деятельности.

При компетентностном подходе результатом образования будет совокупность традиционных результатов образования (ЗУН-ов) с дополнением результатов по становлению и