Практическая работа № 16

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Цель работы. Научиться определять критерии критически важный объект информатизации и их классы.

Краткие сведения из теории

Критически важный объект информатизации (КВОИ) – объект информатизации, который обеспечивает функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение штатного режима которых может привести к чрезвычайной ситуации техногенного характера.

Критически важный объект информатизации (КВОИ) – осуществляет функции информационной системы, нарушение (прекращение) функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

Критически важный объект информатизации (КВОИ) – обеспечивает предоставление значительного объема информационных услуг, частичное или полное прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

Правовые акты, регулирующие КВОИ:

– Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь»;

– Указ Президента Республики Беларусь 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»;

– Постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»;

– Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г. № 42 «Об утверждении Инструкции о порядке проведения внешнего контроля критически важных объектов информатизации»;

– Роль КВОИ определяется указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь».

Основными национальными интересами в информационной сфере является обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Основными потенциальными либо реально существующими угрозами национальной безопасности является нарушение функционирования критически важных объектов информатизации.

В информационной сфере внутренними источниками угроз национальной безопасности является несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Порядок защиты критически важных объектов информатизации по отраслевому принципу основывается на нормативных правовых актах и технических нормативных правовых актах в области защиты информации и включает:

– отнесение объекта информатизации к КВОИ в соответствии с перечнем отраслевых критериев отнесения объектов информатизации к критически важным объектам информатизации;

– классификацию КВОИ в соответствии с нормативными правовыми актами и техническими нормативными правовыми актами;

– организацию защиты КВОИ в соответствии с присвоенным классом КВОИ, нормативными правовыми актами и техническими нормативными правовыми актами.

Таблица 1 – **Примерный перечень показателей уровня ущерба в случае возникновения угроз различного характера в отношении объекта информатизации**

Показатели ущерба	Уровень ущерба		
	умеренный	высокий	катастрофический
1. Ущерб здоровью людей. Количество людей (КЛ), подвергшихся воздействию	Серьезные повреждения, требующие госпитализации или многократного обращения за медицинской помощью $100 \leq КЛ \leq 1000$	Повреждения с угрозой для жизни, вызывающие необходимость госпитализации $1000 \leq КЛ \leq 10000$	Гибель людей или многочисленные повреждения с угрозой для жизни $КЛ > 10000$
2. Вред, причиненный окружающей среде	Вредное воздействие на окружающую среду носит локальный характер в пределах территории объекта, функциониро-	Вредное воздействие на окружающую среду выходит за границы территории объекта, функционирование которого	Вредное воздействие на окружающую среду имеет трансграничный характер

	вание которого обеспечивается объектом информатизации	обеспечивается объектом информатизации	
3. Снижение качества выполнения основных процессов (заданных целевых функций)	Снижение эффективности выполнения процессов, функций (задач). Невыполнение одной и более основных функций	Ухудшение управляемости объекта, снижение качества обслуживания, не совместимое с установленными требованиями качества	Нарушение основных процессов, срыв задач управления – прекращение функционирования объекта
4. Снижение качества выполняемых процессов смежных зависимых объектов	Умеренное воздействие на важные процессы других объектов в пределах одного района или области (региональный уровень)	Существенное воздействие на функционирование или разрушение других объектов в пределах территории государства (республиканский (государственный) уровень)	воздействие на объекты других государств (трансграничный уровень)
5. Экономический ущерб (ЭУ), в процентах от бюджета административно-территориальной единицы по месту нахождения (регистрации) субъекта хозяйствования	$2,5 < ЭУ \leq 10$	$10 < ЭУ \leq 25$	$ЭУ > 25$

Устанавливаются следующие подклассы объектов в зависимости от организации на них вычислительного процесса:

– **подкласс А** – совокупность объектов информатизации, технические средства которых размещены в пределах одной контролируемой зоны и обработка защищаемой информации осуществляется в пределах области действия комплекса средств безопасности объекта (КСБО) (примеры – Автономная ПЭВМ или ряд автономных ПЭВМ, размещенных в одном помещении; ЛВС; информационная система в виде взаимодействующих между собой ЛВС, автоматизированных рабочих мест и др.);

– **подкласс Б** – совокупность объектов информатизации, технические средства которых размещены в нескольких контролируемых зонах, объединенных открытыми или защищенными каналами передачи данных, и обра-

ботка информации осуществляется в пределах области действия КСБО (пример – ОИ, представляющие собой корпоративную вычислительную сеть, т.е. более двух вычислительных сетей или отдельных ПЭВМ, объединенных между собой защищенными каналами передачи данных);

– **подкласс В** – совокупность объектов информатизации, технические средства которых размещены в одной контролируемой зоне и обработка защищаемой информации осуществляется в пределах области действия КСБО, но один или несколько из совокупности объектов имеет (имеют) каналы обмена информацией, выходящие за пределы контролируемой зоны (пример – ОИ, представляющие собой ЛВС или ПЭВМ, подключенные к сетям общего пользования (например, Интернет), и обрабатывающие защищаемую информацию без ее передачи другим, внешним ОИ).

Устанавливаются следующие классы типовых объектов информатизации, для которых необходимо разработать профили защиты:

– **класс А1** – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к государственным секретам, технические средства которых размещены в пределах одной контролируемой зоны;

– **класс Б1** – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к государственным секретам, технические средства которых размещены в нескольких контролируемых зонах, объединенных защищенными каналами передачи данных;

– **класс В1** – для данного класса профиль защиты не разрабатывается, так как объекты информатизации, обрабатывающие информацию, содержащую сведения, отнесенные в установленном порядке к государственным секретам, не должны иметь каналов обмена информацией за пределами контролируемой зоны;

– **класс А2** – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, технические средства которых размещены в пределах одной контролируемой зоны;

– **класс Б2** – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, технические средства которых размещены в нескольких контролируемых зонах, объединенных защищенными каналами передачи данных;

– **класс В2** – для данного класса профиль защиты не разрабатывается, так как объекты информатизации, обрабатывающие служебную информа-

цию ограниченного распространения, не должны иметь каналов обмена информацией за пределами контролируемой зоны;

– **класс А3** – совокупность объектов информатизации, на которых обрабатывается открытая информация в пределах области действия КСБО, технические средства которых размещены в пределах одной контролируемой зоны;

– **класс Б3** – совокупность объектов информатизации, на которых обрабатывается открытая информация в пределах области действия КСБО, технические средства которых размещены в нескольких контролируемых зонах, объединенных открытыми или защищенными каналами передачи данных;

– **класс В3** – совокупность объектов информатизации, на которых обрабатывается открытая информация в пределах области действия КСБО, технические средства которых размещены в пределах одной контролируемой зоны, но имеющие каналы обмена информацией за пределами контролируемой зоны.

Порядок выполнения работы

1 Определить понятие КВОИ и его роль.

2 Проанализировать для каждого вида угроз уровень ущерба в соответствии с таблицей 1. Результаты анализа оформить в виде таблицы 2.

Таблица 2 – **Определение показателей уровня ущерба для угроз**

Наименование угрозы	Критерий 1	Критерий 2	Критерий 3	Критерий 4

3 Сделать вывод о наиболее критических угрозах.

4 Проанализировать для всего объекта уровень ущерба в соответствии с таблицей 1. Результаты анализа оформить в виде таблицы 3.

Таблица 3 – **Определение показателей уровня ущерба для информационного объекта**

Наименование объекта	Критерий 1	Критерий 2	Критерий 3	Критерий 4

4 Определить к какому классу относится рассматриваемый объект.

5 Сделать вывод о соответствии рассматриваемого объекта к КВОИ.

Содержание отчета

1 Цель работы.

2 Результаты анализа угроз по показателям уровня ущерба (таблица 2).

3 Результаты анализа объекта защиты по показателям уровня ущерба (таблица 3).
4 Класс объекта защиты.
5 Вывод по работе.

Контрольные вопросы

1 Что такое КВОИ?
2 Показатели ущерба при возникновении угроз.
3 Классификация объектов защиты.