МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания
по выполнению лабораторных работ
по дисциплине
«Гуманитарные проблемы обеспечения информационной безопасности»
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2024

1. Цель и задачи изучения дисциплины

Целью освоения дисциплины «Гуманитарные проблемы обеспечения информационной безопасности» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Цель освоения дисциплины заключается в формировании формирование набора общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность:

- знакомство с понятиями национальной безопасности; видами безопасности; информационной безопасности (ИБ) в системе национальной безопасности Российской Федерации; основными понятиями, общеметодологическими принципами теории ИБ;
- анализом угроз ИБ, проблемами информационной войны;
- государственной информационной политикой; проблемами региональной информационной безопасности; видами информации;
- методами и средствами обеспечения ИБ;
- методами нарушения конфиденциальности, целостности и доступности
- причинами, видами, каналами утечки и искажения информации.

В результате освоения дисциплины студенты должны:

Знать:

Способность администрировать подсистемы информационной безопасности объекта защиты

Уметь:

Использует основные знания об угрозах безопасности. Обладает навыками мониторинга функционирования подсистемы ИБ.

Владеть:

навыками мониторинга функционирования подсистемы ИБ.

навыками оценивания роли информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

2. Оборудование и материалы

Для проведения лабораторных занятий необходимо следующее материально-техническое обеспечение: персональный компьютер; проектор; возможность выхода в сеть Интернет для поиска по образовательным сайтам и порталам; интерактивная доска.

3. Наименование лабораторных работ

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Обьем часов	Из них практическая подготовка, часов
	3 семестр		
1	**Тема 1. Информационное общество. Информационная реальность.** Методика построения матрицы состояний информационной безопасности	4	4

2	**Тема 2. Гуманитарные проблемы формирования информационного общества.** Действия органов и должностных лиц по предупреждению разглашения конфиденциальной информации	4	4
3	**Тема 3. Понятие информационной безопасности.** Работа с нормативно-правовыми документами, регламентирующими вопросы правового	4	4
4	**Тема 4. Законодательные основы обеспечения национальной безопасности России в информационной сфере.** Использование специальных психологических методик, уникальных психофизических методов и компьютерных психотехнологий при подборе персонала на работу с конфиденциальной информацией	4	4
5	**Тема 5. Угрозы информационной безопасности на объекте.** Юридические меры охраны конфиденциальных сведений как составная часть корпоративной системы защиты информации	4	4
6	**Тема 6. Информационная безопасность как гуманитарная.** Разработка инструкции по обеспечению сохранности конфиденциальной информации на предприятии	4	4
7	**Тема 7. Принципы комплексной системы защиты информации.** Организация службы безопасности предприятия	4	4
8	**Тема 8. Методы и средства защиты информации**. Системный подход к разработке концепции обеспечения безопасности информационного объекта	4	4
9	**Тема 9. Научные исследования в области информационной.** Аналитический подход к классификации угроз безопасности информационного объекта на основе моделирования нарушителей и их действий	4	4
	Итого за 3 семестр	36	36
	Итого	36	36

Лабораторное занятие №1.
Тема: Методика построения матрицы состояний информационной безопасности

Цель занятия
В результате изучения материала занятия студенты должны знать:
- теоретические основы построения систем организационной защиты информации;
- основы. направления и этапы организационной защиты информации. уметь:
- разрабатывать и анализировать эффективность систем организационной защиты информации
- организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации.

иметь навыки:
- построения формальных моделей систем защиты информации;
- работы с литературой, документацией

Содержание занятия

Вводная часть
Многообразие вариантов построения информационных систем порождает необходимость создания различных систем зашиты, учитывающих индивидуальные особенности каждой из них. Большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том как же приступить к созданию комплексной системы защиты информации для конкретных информационных систем, с учетом присущих им особенностей и условий функционирования.
Вместе с тем, в настоящее время разработано и применяется достаточное количество технологий, способов и средств защиты информации, которые необходимо проанализировать и использовать уже сегодня. Это позволит резко сократить вероятность утечки сведений конфиденциальною характера.
Но как сложить в стройную систему разрозненные знания и частные решения?

1. Основы построения систем защиты информации
Теоретические основы построения систем защиты исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства.
Рассматриваются следующие ОСНОВЫ построения систем защиты информации:
- Законодательная, нормативно-методическая и научная база;
- Структура и задачи органов (подразделений), осуществляющих комплексную защиту информации;
- Организационно-технические и режимные меры (политика информационной безопасности);
- Программно-технические методы и средства защиты информации.

Целевая установка теоретических основ заключается в разработке и научном обосновании принципов и методов оптимизации мероприятий по ЗИ. Основной способ достижения указанной цели заключается в решении следующих задач:
- создание предпосылок для реализации упреждающей стратегии ЗИ;
- разработка регулярных методик оценки уязвимости информации и требуемого уровня ее защиты; синтеза оптимальных систем ЗИ;
- обоснование необходимой инфраструктуры ЗИ в общегосударственном масштабе.

2. Направления создания систем защиты информации
Большое число различных компонентов, операций, ресурсов и объектов ИС создает весьма привлекательную среду для различного рода вторжений и несанкционированных операций.

В этой части ИС как объект защиты рассматривается по следующим направлениям:

- Защита информационных и физических объектов информационных систем;
- Техническая защита информации на объектах ИС;
- Зашита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

Рассматривая ИС как объект защиты, обращается внимание на следующие характеристики, влияющие на безопасность информации:

- категории обрабатываемой в ИС информации, высший гриф секретности информации;
- общая структурная схема и состав ИС (перечень и состав оборудования, технических и программных средств, пользователей, данных и их связей, особенности конфигурации и архитектуры и т.п.);
- тип ИС (одно- либо многопользовательская система, открытая сеть, одно- либо многоуровневая система и т.п.);
- объемы основных информационных массивов и потоков,
- производительность системы при решении функциональных задач,
- процедуры восстановления работоспособности после сбоев, наличие средств повышения надежности и живучести и т.п.;
- технические характеристики используемых каналов связи (пропускная способность, типы кабельных линий, виды связи с удаленными сегментами ИС и пользователями и т.п.);
- территориальное расположение компонентов ИС, их физические параметры и т.п.;
- наличие особых условий эксплуатации и др.

3. Этапы создания систем защиты информации

В этой части рассмотрим следующие ЭТАПЫ создания СЗИ:

- Определение информационных и технических ресурсов, а также объектов ИС подлежащих защите;
- Выявление полного множества потенциально возможных угроз и каналов утечки информации;
- Проведение оценки уязвимости и рисков информации (ресурсов ИС) при имеющемся множестве угроз и каналов утечки;
- Определение требований к системе защиты информации;
- Осуществление выбора средств защиты информации и их характеристик;
- Внедрение и организация использования выбранных мер, способов и средств защиты;
- Осуществление контроля целостности и управление системой защиты.

4. Конкретные решения и рекомендации...

В этой части рассмотрим описания конкретных подходов, разработок и изделий различных фирм и организаций, работающих в области проблем защиты информации. Как известно, для того чтобы решить проблему надо быть выше нее и немного в стороне. Обратите внимание на рисунок 1.

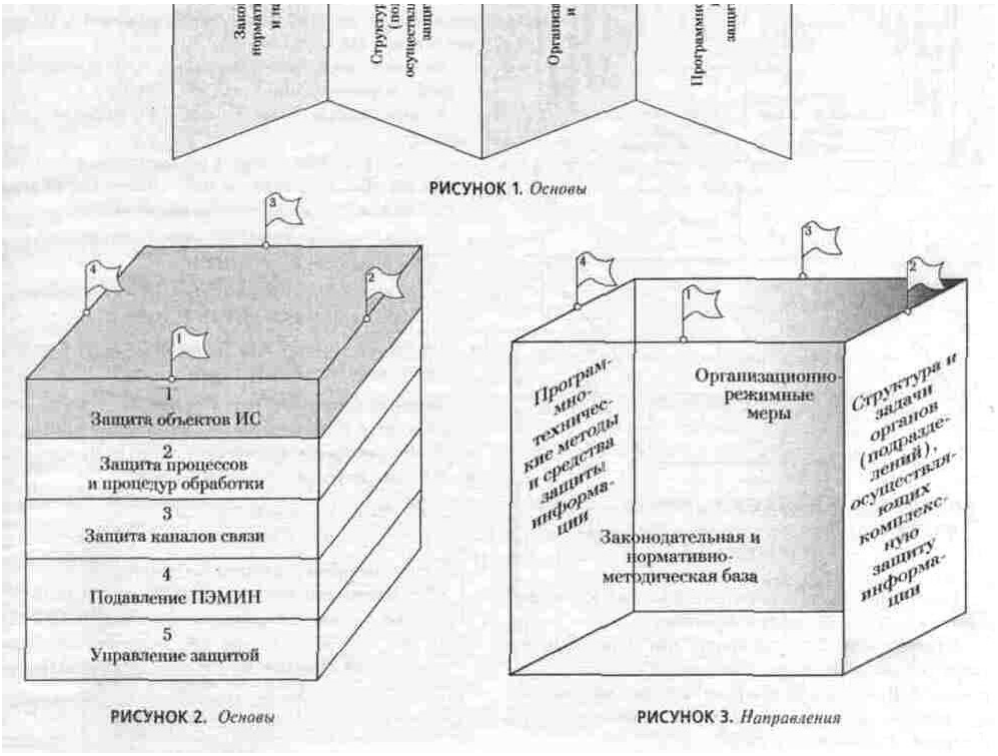


РИСУНОК 1. *Основы*

РИСУНОК 2. *Основы*

РИСУНОК 3. *Направления*

Известно, что ***ОСНОВОЙ*** или составными частями практически любой ***СИСТЕМЫ*** (в том числе и системы защиты информации) являются:

1. Законодательная, нормативно-правовая и научная база;
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ;
3. Организационно-технические и режимные меры и методы (политика информационной безопасности);
4. Программно-технические способы и средства.

Представим ***ОСНОВЫ*** в виде куба, внутри которого и находятся все вопросы (предметная область) защиты информации (Рис.2).

Далее, руководствуясь принципом декомпозиции, выделим основные ***НАПРАВЛЕНИЯ*** в общей проблеме обеспечения безопасности информационных технологий (они представлены на Рис. 3).

НАПРАВЛЕНИЯ формируются исходя из конкретных особенностей ИС как объекта защиты. В общем случае, исходя из типовой структуры ИС и исторически сложившихся видов работ по защите информации предлагается рассмотреть следующие направления:

1. Защита объектов информационных систем;
2. Защита процессов, процедур и программ обработки информации;
3. Защита каналов связи;
4. Подавление побочных электромагнитных излучений.
5. Управление системой защиты;

Но поскольку каждое из этих направлений базируется на перечисленных выше ***ОСНОВАХ***, то грани куба объединяют ***ОСНОВЫ и НАПРАВЛЕНИЯ*** неразрывно связанные друг с другом (см. Рис. 3). Но это еще не все... Далее рассматриваются ***ЭТАПЫ*** (последовательность шагов) построения **СЗИ** (см. Рис. 4), которые необходимо пройти в равной степени для всех и каждого в отдельности ***НАПРАВЛЕНИЙ*** (с учетом всех ОСНОВ).

РИСУНОК 4. *Применение МЕТОДИКИ для каждого из НАПРАВЛЕНИЙ с учетом общего представления структуры СЗИ.*

Проведенный анализ существующих методик (последовательностей) работ по созданию СЗИ позволяет выделить следующие ***ЭТАПЫ***:

1. Определение информационных и технических ресурсов, а также объектов ИС(!) подлежащих защите;
2. Выявление полного множество потенциально возможных угроз и каналов утечки информации;
3. Проведение оценки уязвимости и рисков информации (ресурсов ИС) при имеющемся множестве угроз и каналов утечки;
4. Определение требований к системе защиты информации;
5. Осуществление выбора средств защиты информации и их характеристик;
6. Внедрение и организация использования выбранных мер, способов и средств защиты.
7. Осуществление контроля целостности и управление системой защиты.

Указанная последовательность действий осуществляется непрерывно по замкнутому циклу, с проведением соответствующего анализа состояния СЗИ и уточнением требований к ней после каждого шага.

Последовательность прохождения ЭТАПОВ создания СЗИ для каждого из НАПРАВЛЕНИЙ с учетом ОСНОВ (структуры СЗИ) условно показано на Рис.4.

Матрица знаний информационной безопасности

А теперь развернем этот кубик на плоскости. Получится трехмерная матрица или попросту таблица, которая поможет систематизировать материал.

СЗИ лишь тогда станет системой, когда будут установлены логические связи между всеми се составляющими. Как же организовать такое взаимодействие?

МАТРИЦЫ СОСТОЯНИЙ -своего рода таблица, позволяющая логически объединить составляющие блоков "ОСНОВЫ", "НАПРАВЛЕНИЯ" и "ЭТАПЫ" по принципу каждый с каждым.

Напомним, что матрица появляется не сама по себе, а формируется в каждом конкретном случае, исходя из конкретных задач по созданию конкретной СЗИ для конкретной ИС.

Наглядно процесс формирования СЗИ с использованием матрицы знаний изображен на Рис. 5.

РИСУНОК 5. *Структурная схема формирования СЗИ с помощью матрицы знаний.*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	Базы	Структуры	Меры	Средства	Базы	Структуры	Меры	Средства	Базы	Структуры	Меры	Средства	Базы	Структуры	Меры	Средства	Базы	Структуры	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 6. *Нумерация элементов матрицы знаний.*

Рассмотрим как можно использовать предложенную матрицу.
Элементы матрицы имеют соответствующую нумерацию (см. Рис.6.) Следует обратить внимание на обозначения каждого из элементов матрицы, где:

- первое знакоместо (X00) соответствует номерам составляющих блока "ЭТАПЫ",
- второе знакоместо (0X0) соответствует номерам составляющих блока "НАПРАВЛЕНИЯ",
- третье знакоместо (00X) соответствует номерам составляющих блока "ОСНОВЫ".

Такая же нумерация используется в названиях разделов, глав и вопросов, рассматриваемых в книге.
В общем случае количество элементов матрицы может быть определено из соотношения $K = O_i * H_j * M_k$, где
К — количество элементов матрицы
O_i — количество составляющих блока "ОСНОВЫ"
H_j — количество составляющих блока "НАПРАВЛЕНИЯ"' M_k — количество составляющих блока "ЭТАПЫ"
В нашем случае общее количество элементов "матрицы" равно 140 К =4*5*7= 140
Представление элементов матрицы
Содержание каждого из элементов МАТРИЦЫ описывает взаимосвязь составляющих создаваемой СЗИ. Перечень вопросов описывающих каждый из элементов матрицы, приведен далее.
Комплекс вопросов создания и оценки СЗИ рассматривается путем анализа различных групп элементов матрицы, в зависимости от решаемых задач.

Например, отдельно можно оценить качество нормативной базы (Рис.7) или защищенность каналов связи (Рис.8), или качество мероприятий по выявлению каналов утечки информации (Рис.9) т.д.

РИСУНОК 7

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 8

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 9

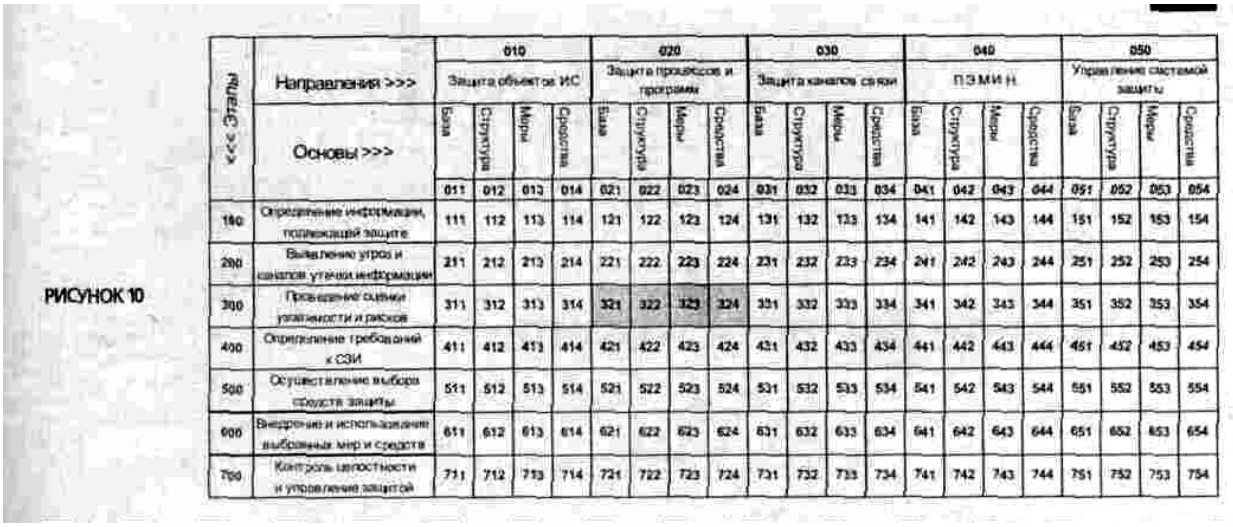
<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

В общем случае рассматриваются все 140 вопросов (по числу элементов матрицы). Описание этих вопросов позволяют составить полное представление о СЗИ и оценить достигнутый уровень защиты.

В общем случае основным содержанием элементов матрицы является ответ на вопрос "Какие из мероприятий по защите информации, кем и как выполняются?"

В другом примере на Рис.10 приведено содержание для элементов № 321, 322, 323, 324, которые объединяют следующие составляющие:

РИСУНОК 10



<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П.Э.М.И.Н.				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

- № 3 (300 проведение оценки уязвимости и рисков) блока "ЭТАПЫ",
- № 2 (020 защита процессов и программ) блока "НАПРАВЛЕНИЯ"
- № 1, 2. 3, 4 (001 нормативная база, 002 структура органов, 003 мероприятия, 004 используемые средства) блока "ОСНОВЫ".

Опишем содержание информации в указанных элементах матрицы.
Вот что получилось:

- Элемент № 321 содержит информацию о том насколько полно отражены в законодательных, нормативных ч методических документах вопросы, определяющие порядок проведения оценки уязвимости и рисков для информации используемой в процессах и программах конкретной ИС?
- Элемент № 322 содержит информацию о том имеется ли структура органов (сотрудники), ответственная за проведение оценки уязвимости и рисков для процессов и программ ИС?
- Элемент № 323 содержит информацию о том определены ли режимные меры. обеспечивающие своевременное и качественное проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?
- Элемент № 324 содержит информацию о том применяются ли технические, программные или другие средства, для обеспечения оперативности и качества проведения оценки уязвимости и рисков в процессах и программах И С?

Это содержание только четырех вопросов из ста сорока, но ответы на них уже позволяют сформировать некое представление о состоянии дел по защите информации в конкретной ИС.

Отчетность за занятие

Каждый студент должен оформить в отдельной тетради матрицу состояний информационной безопасности с описанием всех ее элементов и защитить методику у преподавателя.

Лабораторное занятие №2.
Тема: Действия органов и должностных лиц по предупреждению разглашения конфиденциальной информации

Цель занятия

В результате изучения учебного материала студенты должны
знать:
- способы разглашения;
- особенности и условия разглашения;
- классификацию организационных каналов утечки конфиденциальной информации.
- направления работы с кадрами в интересах формирования у них умения хранить тайну и строго соблюдать установленные правила работы с закрытой информацией.

уметь:
- организовывать работу на предприятии по предупреждению разглашения;
- организовывать и проводить аналитическую работу по предупреждению разглашения конфиденциальной информации.

вопросы:
1. Понятие разглашения конфиденциальной информации
- способы разглашения;
- особенности и условия разглашения;

2. Мероприятия по предупреждению разглашения конфиденциальной информации:
- действия органов и должностных лиц по предупреждению разглашения конфиденциальной информации

1. Понятие разглашения конфиденциальной информации

Исходя из поговорки «болтун — находка для шпиона», следует учесть, что из всех условий, способствующих неправомерному овладению конфиденциальной информацией, излишняя болтливость собственных сотрудников фирмы составляет 32%. Это третья часть. Если еще добавить, что безответственный обмен опытом составляет 2%, то получается, что разглашение коммерческих секретов составляет почти половину (42%) угроз конфиденциальной информации!

Умышленное разглашение производственных секретов обходится экономике США в 2 миллиарда долларов ежемесячно. Как установило в ходе недавнего опроса предприятий американское общество промышленной безопасности (АСИС), **число** подобных инцидентов с 1993 года утроилось.

Причин этого роста несколько. Лояльность одних служащих подрывает ужесточение дисциплины, других - перекупают конкуренты. Это касается в первую очередь высокотехнологичных отраслей.

К конкурентам частенько попадают материалы о стратегии предприятий, результаты исследовательских и опытно-конструкторских работ, списки клиентов, заявки на патенты, торговые марки и авторские права.

Общие положения

Разглашение - это умышленные или неосторожные действия должностных лиц и граждан, результатом которых явилось неправомерное оглашение конфиденциальных сведений, и как следствие — ознакомление с ними лиц, не допущенных к этим сведениям. Выражается разглашение в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и иных способах обмена деловой и научной информацией.

С точки зрения инициативы образование информационного контакта и степени участия в нем компонентов коммуникации активной стороной выступает источник, т. е. владелец информации.

Считается, что разглашение охраняемой информации может произойти при наличии ряда условий и обстоятельств служебного и личного характера. Причины разглашения, как правило, связаны с несовершенством
разработанных норм по защите информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами и сведениями, содержащими конфиденциальную информацию.
К факторам и обстоятельствам, приводящим к разглашению информации, относятся (Рис.1):

- недостаточное знание сотрудниками правил защиты конфиденциальной информации и непонимание (или недопонимание) необходимости тщательного их выполнения;
- слабый контроль за соблюдением правил работы со сведениями конфиденциального характера;
- текучесть кадров, в том числе знающих сведения конфиденциального характера

Разглашение конфиденциальной информации возможно:

1. При передаче информации по каналам электросвязи.
2. При сообщении, оглашении:
   - на деловых встречах и переговорах;
   - при деловой переписке;
   - на семинарах, симпозиумах, в печати и СМИ;
   - на выставках;
   - в судебных инстанциях и административных органах.
3. При пересылке документов:
   - по каналам почтовой связи;
   - нарочными, курьерами, попутчиками.
4. При опубликовании:
   - в печати;
   - в научных исследованиях и диссертациях.
5. При личном общении:
   - на встречах;
   - при телефонных переговорах.
6. При утере, утрате документов:

- на работе;
- за пределами службы.

7. При бесконтрольном оставлении документов:
- на рабочем месте;
- на экране ПЭВМ;
- при ксерокопировании.

8. При бесконтрольной разработке документов:
- необоснованное изготовление документов;
- включение в обычные документы сведений конфиденциального характера;
- черновики, наброски, испорченные варианты.

9. При бесконтрольном документообороте:
- необоснованная рассылка документов;
- необоснованное ознакомление с документами сотрудников и соисполнителей.

10. При бесконтрольном хранении и уничтожении документов.

11. При бесконтрольном приеме поступающей документации.

Известны формальные и неформальные **каналы** распространения информации (рис.2)

В жизни таких условий и направлений значительно больше и рассматривать их необходимо на конкретных объектах.

<u>В основу защиты информации от разглашения целесообразно положить:</u>

1. Принцип максимального ограничения числа лиц, допущенных к работе с конфиденциальной информацией, так как степень ее сохранности находится в прямой зависимости от числа допущенных к ней лиц.

2. Принцип персональной ответственности за сохранность информации предполагает разработку мер, побуждающих сотрудников хранить секреты не только из-за боязни последствий за вольное или невольное раскрытие, но и обеспечивающих заинтересованность каждого конкретного работника в сохранении тайны.

Отсюда одним из направлений работы является работа с кадрами, воспитательно-профилактическая деятельность, которая включает в себя совокупность методов воздействия на сознание, чувство, волю и характер сотрудников в интересах

формирования у них умения хранить тайну и строго соблюдать установленные правила работы с закрытой информацией.

Главные направления этой деятельности:

- привитие навыков предупреждения **разглашения** конфиденциальной информации;
- повышение ответственности за сохранение секретов;
- создание обстановки нетерпимости к фактам нарушения установленного порядка обеспечения информационной безопасности;
- строгий контроль за всеми видами переговоров со сторонними организациями и их представителями;
- контроль публикаций, выступлений, интервью и других форм общения по вопросам деятельности предприятия;
- контроль разговоров в служебных помещениях и телефонных переговоров сотрудников на служебные темы;
- изучение действий и поведения сотрудников во внеслужебное время, мест их пребывания, наклонностей, увлечений, пагубных привычек, трудового удовлетворения и другие.

Естественно, что все эти действия должны проводиться в строгом соответствии с законодательными актами, с точным соблюдением прав и обязанностей сотрудников предприятия, без какого-либо вмешательства в личную жизнь.

Подобные действия могут выполнять, например, частные детективы (сотрудники службы безопасности). Согласно Закону РФ «О частной детективной и охранной деятельности», им разрешается осуществлять следующие виды услуг:

1. Сбор сведений по гражданским делам.
2. Изучение рынка.
3. Сбор сведений о партнерах и конкурентах.
4. Выявление недобросовестных и неплатежеспособных партнеров.
5. Установление обстоятельств недобросовестной конкуренции.
6. Установление обстоятельств разглашения коммерческих секретов. Эти услуги реализуются с целью:

1. Поиска без вести пропавших.
2. Поиска утраченного имущества.
3. Выявления биографических данных, характеризующих граждан.
4. Изучения сведений по уголовным делам и другое. При этом частному детективу разрешается:

1. Устный опрос граждан и должностных лиц с **их** согласия.
2. Изучение предметов и документов с согласия **их** владельцев.
3. Наведение справок.
4. Внешний осмотр помещений и других объектов.
5. Наблюдение для получения необходимой информации.
6. Использование видео- и аудиозаписи, кино- и фотосъемки, технических и иных средств, не причиняющих вреда гражданам, оперативной связи.
7. Использование специальных средств личной безопасности.

Опыт работы по пресечению разглашения конфиденциальной информации позволяет разработать определенную систему мер по предотвращению разглашения на общем уровне рекомендаций в виде типового классификатора защитных действий по предотвращению разглашения конфиденциальной информации. Такой документ может быть детальным, если он будет привязан к конкретному объекту с акцентом на местные условия, учетом имеющихся средств, особенностей зданий и помещений.

В качестве примера для изучения рассмотрим вариант «Каталога защитных действий по пресечению разглашения конфиденциальной информации» на общем уровне рекомендаций.

С целью придания «Каталогу» практической значимости в интересах повседневного использования служба безопасности должна внести в него конкретные мероприятия с привязкой к конкретным условиям.

КАТАЛОГ обобщенных мероприятий по защите конфиденциальной информации

В каталоге (В. И. Ярочкин, 2000) рассматриваются обобщенные мероприятия по защите конфиденциальной информации от разглашения, утечки по техническим каналам и от несанкционированного доступа со стороны злоумышленников, конкурентов и иных субъектов противоправных интересов.

Каталог состоит их трех разделов:

1. Мероприятия по предупреждению разглашения конфиденциальной информации.
2. Мероприятия по защите информации от утечки по техническим каналам.
3. Мероприятия по пресечению несанкционированного доступа к конфиденциальной информации.

А). Мероприятия по предупреждению разглашения конфиденциальной информации

РАЗГЛАШЕНИЕ — умышленные неосторожные действия должностных лиц и граждан, приводящие к оглашению конфиденциальной информации, доверенной им по службе, и ознакомлению с ней лиц, не имеющих на это права.

РАЗГЛАШЕНИЕ выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и других способах и реализуется по каналам распространения и средствам массовой информации.

ПРЕДУПРЕЖДЕНИЕ РАЗГЛАШЕНИЯ — это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого оглашения конфиденциальной информации.

Деятельность руководства предприятия и сотрудников службы безопасности по предупреждению разглашения охраняемых сведений включает в себя и обучение сотрудников, ознакомление их с законами,

постановлениями, положениями, инструкциями, определяющими правовое отношение с государством и предприятием.

Значительное место в работе с персоналом должно отводиться обучению методам и мерам обеспечения сохранности ценной информации. В процессе обучения необходимо добиваться, чтобы сотрудники четко знали категории охраняемых ими сведений, ценность этих данных, возможные способы и мето- ды проникновения со стороны нарушителей, а также правила и процедуры их защиты. Следует особо обратить внимание на то, чтобы сотрудники осознанно понимали разумность и необходимость всех действующих элементов режима сохранения секретов.

Следует использовать любую возможность для пропаганды обеспечения экономической безопасности предприятия; не забывать периодически вознаграждать сотрудников фирмы за успехи в этой работе; всемерно стимулировать заинтересованность и участие сотрудников в выполнении программы по обеспечению безопасности.

Важной составляющей обеспечения информационной безопасности фирмы является контроль лояльности ее персонала. Такая работа проводится как в целях упреждения преступных посягательств, так и для расследования конкретных случаев нанесения ущерба.

Неотъемлемая часть этой работы — мониторинг телефонных переговоров, ведущихся из офиса. Осуществляется также акустический или визуально-акус- тический контроль разговоров и действий в служебных помещениях.

Понимая всю важность соблюдения конфиденциальности мониторинга телефонных переговоров в пределах конкретного предприятия, Правительством РФ 22 марта 1995 г. было принято Постановление № 291, в котором указывается: «Лица, участвующие в

мониторинге, обязаны сохранять государственную и коммерческую тайну, к которой они получили доступ».

Сейчас магнитные фонограммы прочно вошли в уголовный процесс как вещественное доказательство. Суды всех без исключения инстанций (в том числе и с участием присяжных заседателей) принимают магнитные фо- нограммы как неоспоримое доказательство по делу.

Экспертизу подлинности зафиксированной на пленке информации проводят эксперты экспертно-криминалистического центра МВД России. Почти во всех МВД, УВД созданы лаборатории видеофоноскопических экспертиз и исследований.

Выводы

1. Разглашение конфиденциальной информации является наиболее распространенным действием, приводящим к неправомерному оглашению охраняемых сведений.
2. К факторам и обстоятельствам, приводящим к разглашению информации, относятся:

• недостаточная подготовленность сотрудников к соблюдению требований по защите конфиденциальной информации;

• слабый контроль со стороны руководства и соответствующих служб за установленным порядком защиты информации.

3. Основными направлениями деятельности по пресечению разглашения охраняемых сведений являются правовые и организационные меры **по** повышению ответственности сотрудников к соблюдению установленных мер и требований **по** защите конфиденциальной информации.

Вопросы для контроля знаний студентов

1. Раскройте направления возможных КУ ОИ через каналы оперативной связи.
2. Формальные каналы распространения информации.
3. Неформальные каналы распространения информации.
4. Какие факторы и обстоятельства приводят к разглашению информации?
5. Назовите направления работы с кадрами в интересах формирования у них умения хранить тайну и строго соблюдать установленные правила работы с закрытой информацией.
6. Назовите КУ ОИ при ведении секретного и открытого делопро- изводства.
7. Какие организационные меры следует предпринять, чтобы уменьшить утечку ОИ через разглашение?

Основная литература

1. Организация и современные методы защиты информации /Под общей редакцией Диева С.А., Шаваева А.Г./, М.: Концерн «Банковский Деловой Центр», 2013, 472с.
2. Петрков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 2013, 568с.
3. Нормативные правовые акты по защите государственной тайны. Часть 1. М.: СИП РИА, 2014, 132с.
4. Нормативные правовые акты по защите государственной тайны. Часть П. М.: СИП РИА, 2013, 56с.
5. Ярочкин В.И. Служба безопасности коммерческого предприятия. Организационные вопросы. М.: «Ось-89», 2021.
6. Барсуков **В.С.,** Марущенко В.В., Шигин В.А. Интегральная безопасность: Информационно-справочное пособие. - М.: РАО "Газпром", 2014.- 170с.
7. В.А. Северин Правовое обеспечение информационной безопасности предприятия: Учебно-практическое пособие. М.: Городец, 2021. -192 с.
8. Брусницин Н.А. Открытость и шпионаж. - М.: Воениздат, 2013-56с.
9. Мироничев С. Коммерческая разведка или промышленный шпионаж в России и

методы борьбы с ним. - М.: Дружок, 2021. -223с.
10. Поздняков Е. Утечка информации // Секьюрити. - 2021. -№5.-С. 28...29.
11. Поляков А.В. Промышленный шпионаж и как с ним бороться.// Мы и безопасность. 2014. - № 2. - С. 22...44.
12. Терминология в области защиты информации: Справочник. - М.: ВНИИ "Стандарт", 2013. - 110 с.

ПЕРИОДИЧЕСКИЕ ИЗДАНИЯ:

Журналы - “Мир безопасности»; Защита информации “Конфидент”; “Безопасность информации”; “Безопасность достоверности информации”; «Бизнес и безопасность в России»; «Вопросы защиты информации».

Газеты “Коммерсант”, “Российская газета”.

Лабораторное занятие №3.
Тема: Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования допуска и доступа граждан к государственной тайне

Цели:

1. В результате изучения материала занятия студенты должны:

знать

- Постановление Правительства РФ от 28 октября 1995 г. N 1050 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
- Перечень медицинских противопоказаний для осуществления работы с использованием сведений, составляющих государственную тайну, утвержден приказом Минздрава РФ от 16 марта 1999 г. N 83
- Общие положения Инструкции "о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
- Порядок допуска и доступа к государственной тайне.

уметь

правильно заполнять следующие формы документов по защите ГТ:

- Форма 1 Номенклатура должностей работников, подлежащих оформлению на допуск к особой важности, совершенно секретным и секретным сведениям;
- Форма 2 Анкета;
- Форма 3 Карточка;
- Форма 4 Список на оформляемого гражданина и его близких родственников
- Форма 5 Учетная карточка на допуск по первой и второй формам
- Форма 6 Список лиц, подлежащих допуску к секретным сведениям по указанной организации;
- Форма 7 Отметка органов ФСБ России о проведении проверочных мероприятий для оформления допуска по третьей форме;
- Форма 8 Карточка на допуск по третьей форме;
- Форма 9 Типовой договор(контракт) об оформлении допуска к государственной тайне (приложение к трудовому договору);
- Форма 10 Журнал учета карточек на допуск работников по первой и второй формам;
- Форма 11 Справка о допуске по первой форме;
- Форма 12 Справка о допуске по второй форме;
- Форма 13 Справка о допуске по третьей форме;
- Форма 14 Журнал учета выдачи справок о допуске;
- Форма 15 Карточка учета выдачи справок о допуске;
- Форма 16 Предписание на выполнение задания;
- Форма 17 Журнал учета командированных

Иметь представление

- о порядке доступа граждан к особой важности, совершенно секретным и секретным сведениям при командировании их в другие организации;
- о "Положении о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне" (утв. постановлением Правительства РФ от 22 августа 1998 г. N 1003)

2. Прививать студентам навыки исследовательского подхода к изучению дисциплины.
3. В ходе изложения материала показать взаимосвязь общенаучных и ОПФ дисциплин.

Вопросы для контрольного опроса:

1. Перечислите субъекты и объекты правоотношений в сфере защиты государственной тайны.
2. Раскройте принципы засекречивания.
3. Каковы особенности механизма засекречивания?
4. Дайте сравнительный анализ механизмов засекречивания в России и США.
5. Каковы реквизиты носителей государственной тайны?
6. В чем заключаются особенности рассекречивания?
7. Какова система органов защиты государственной тайны, каковы основные правомочия включенных в нее органов государственной власти?
8. Перечислите основные правовые механизмы допуска граждан к ГТ.
9. В чем заключается и из чего состоит механизм распоряжения ГТ?

СОДЕРЖАНИЕ ЗАНЯТИЯ

1. Порядок допуска и доступа к ГТ. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.

Постановление Правительства РФ от 28 октября 1995 г. N 1050
"Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"

В соответствии с Законом Российской Федерации "О государственной тайне" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемую Инструкцию о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне.
2. Федеральной службе безопасности Российской Федерации совместно с заинтересованными федеральными органами исполнительной власти в 3- месячный срок разработать комплекс мер организационного, материально- технического и иного характера, необходимых для проведения работ по допуску должностных лиц и граждан Российской Федерации к государственной тайне.
3. Признать утратившим силу постановление Правительства Российской Федерации от 22 декабря 1992 г. N 1025-69.

Считать не действующим на территории Российской Федерации раздел 3 Инструкции по обеспечению режима секретности в министерствах, ведомствах, на предприятиях, в учреждениях и организациях СССР, утвержденной постановлением Совета Министров СССР от 12 мая 1987 г. N 556-126.

I. Общие положения

1. Инструкция разработана в соответствии с Законом Российской Федерации "О государственной тайне", другими актами действующего законодательства, которые регулируют отношения, связанные с защитой государственной тайны, и определяет порядок допуска должностных лиц и граждан Российской Федерации (далее именуются - граждане) к государственной тайне. Ее положения обязательны для выполнения органами государственной власти Российской Федерации, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы, которые выполняют работы, связанные с использованием сведений, составляющих государственную тайну, либо стремятся в установленном порядке получить лицензию на право проведения таких работ.

Федеральным законом *от 6 октября 1997 г. N 131-ФЗ установлен особый порядок допуска к государственной тайне членов Совета Федерации,*
депутаты Государственной Думы, судей на период исполнения ими своих полномочий,

адвокатов, участвующих в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну

2. В федеральных органах исполнительной власти в соответствии с требованиями настоящей Инструкции, особенностями деятельности и характером выполняемых задач при необходимости могут разрабатываться ведомственные инструкции, которые согласовываются с Федеральной службой безопасности Российской Федерации и утверждаются руководителями этих органов.

3. Допуск граждан к государственной тайне на территории Российской Федерации и за ее пределами осуществляется руководителями соответствующих организаций в порядке, установленном настоящей Инструкцией.

Граждане, которым по характеру занимаемой ими должности необходим доступ к государственной тайне, могут быть назначены на эти должности только после оформления допуска по соответствующей форме в установленном порядке.

Руководители организаций несут персональную ответственность за подбор лиц, допускаемых к сведениям, составляющим государственную тайну, а также за создание условий, при которых граждане знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые в соответствии со статьей 25 Закона Российской Федерации "О государственной тайне" необходимы для выполнения ими должностных (функциональных) обязанностей.

4. В соответствии со статьей 21 Закона Российской Федерации "О государственной тайне" допуск граждан к государственной тайне осуществляется в добровольном порядке и предусматривает:

принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

согласие на частичные временные ограничения их прав в соответствии со статьей 24 указанного Закона;

письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

определение видов, размеров и порядка предоставления льгот, предусмотренных указанным Законом;

ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

принятие соответствующего решения руководителем организации о допуске оформляемого лица к государственной тайне.

Взаимные обязательства администрации организации и оформляемого лица отражаются в трудовом договоре (контракте). Заключение трудового договора (контракта) до окончания проверочных мероприятий не допускается.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо.

5. Основанием для отказа гражданину в допуске к государственной тайне в соответствии со статьей 22 Закона Российской Федерации "О государственной тайне" могут являться:

признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;

наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения и медицинской промышленности Российской Федерации;

Перечень *медицинских противопоказаний для осуществления работы с использованием сведений, составляющих государственную тайну, утвержден* приказом *Минздрава РФ от 16 марта 1999 г. N 83*

постоянное проживание его самого и (или) его близких родственников за границей и (или)

оформление указанными лицами документов для выезда на постоянное место жительства в другие государства;
выявление в результате проведения проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;
уклонение от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.
Решение об отказе гражданину в допуске к государственной тайне принимается руководителем организации в индивидуальном порядке с учетом результатов проверочных мероприятий. Гражданин имеет право обжаловать это решение в вышестоящую организацию или в суд.

6. В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:
первая форма - для граждан, допускаемых к сведениям особой важности;
вторая форма - для граждан, допускаемых к совершенно секретным сведениям;
третья форма - для граждан, допускаемых к секретным сведениям.
Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности Российской Федерации и ее территориальными органами (далее именуются - органы безопасности) во взаимодействии с органами, осуществляющими оперативно-розыскную деятельность.
Допуск граждан по третьей форме, за исключением случая, указанного в пункте 26 настоящей Инструкции, осуществляется руководителем организации без проведения проверочных мероприятий органами безопасности.
Органы безопасности во взаимодействии с заинтересованными организациями имеют право определять те организации, на которых допуск к секретным сведениям осуществляется только после проведения проверочных мероприятий органами безопасности.
Руководители организаций допускаются к секретным сведениям (по третьей форме) только после проведения проверочных мероприятий органами безопасности.
Руководители организаций обязаны осуществлять контроль за соответствием формы допуска граждан степени секретности сведений, к которым они фактически имеют доступ.

7. Граждане, принимаемые на временную работу или не достигшие 18- летнего возраста, как правило, не подлежат оформлению на допуск к особой важности и совершенно секретным сведениям, за исключением случаев, предусмотренных пунктами 27 и 28 настоящей Инструкции.

8. Граждане, принимаемые на работу в подразделения по защите государственной тайны, а также для ведения секретного делопроизводства в организациях, где штатным расписанием не предусмотрено наличие таких подразделений, оформляются на допуск по второй форме, если по характеру выполняемой работы им не требуется допуск по первой форме.

9. Решение о допуске военнослужащих и гражданского персонала военного представительства к государственной тайне принимается руководителем этого военного представительства, который обязан письменно сообщить в подразделение по защите государственной тайны организации по месту аккредитации военного представительства форму и номер допуска этих лиц, а также дату окончания проведения проверочных мероприятий. При отсутствии в военном представительстве подразделения по защите государственной тайны оформление допуска сотрудникам может производиться подразделением по защите государственной тайны организации по месту аккредитации военного представительства.
Граждане, работающие в филиалах организаций (обособленных подразделениях, постоянно действующих экспедициях и т.п.) и постоянно проживающие по месту их нахождения, оформляются на допуск к особой важности, совершенно секретным и секретным сведениям руководителями этих филиалов (подразделений, экспедиций и т.п.).

Проверочные мероприятия в этом случае осуществляются органами безопасности по месту расположения (республика, край, область) этих объектов.

10. Военнослужащие военно-строительных отрядов в случае их привлечения организациями к выполнению совершенно секретных строительно-монтажных работ допускаются к таким работам руководителями этих организаций только после проведения проверочных мероприятий органами безопасности и оформления в установленном порядке допуска по второй форме.

Указанные военнослужащие допускаются на техническую территорию режимных объектов *(1) для проведения секретных и несекретных работ на основании справок о допуске по третьей форме, выданных командованием.

11. Граждане, командируемые на любой срок для работы в российских организациях за рубежом (посольствах, представительствах при международных организациях, консульствах, торговых представительствах и т.п.), в период пребывания за границей допускаются при необходимости к секретным сведениям руководителями этих организаций.

Члены экипажей судов загранплавания и другие граждане, имеющие допуск для работы на таких судах, могут допускаться к совершенно секретным и секретным сведениям капитанами судов только в тех объемах, которые необходимы для выполнения ими должностных (функциональных) обязанностей.

12. Члены поездных бригад, экипажей судов морского и речного флота и иных транспортных средств (кроме транспортных средств Вооруженных Сил Российской Федерации), занимающихся специальными перевозками, буксировкой секретных изделий или совершающих рейсы на режимные объекты, получают допуск по третьей форме, а командный состав указанных бригад и экипажей - по второй форме. Начальники поездных бригад железнодорожных составов, командный состав экипажей судов морского и речного флота и иных транспортных средств, не занимающихся специальными перевозками и буксировкой секретных изделий, в пределах выполнения ими должностных (функциональных) обязанностей получают допуск к секретным сведениям по третьей форме.

13. Перечень должностей, при назначении на которые граждане обязаны оформлять допуск к сведениям, составляющим государственную тайну, определяется номенклатурой должностей (форма 1), утверждаемой руководителем организации или его заместителем, занимающимся вопросами защиты государственной тайны, после согласования ее с органом безопасности. В номенклатуру включаются только те должности, по которым допуск граждан к указанным сведениям действительно необходим для выполнения ими должностных (функциональных) обязанностей.

В номенклатуру могут включаться должности работников, допуск которых к сведениям соответствующей степени секретности обусловлен выполнением ими заданий в других организациях, куда они командируются на основании распоряжений вышестоящих организаций, соглашений или договоров, предусматривающих выполнение совместных работ.

Изменения и дополнения в номенклатуру должностей вносятся по мере необходимости, согласовываются и утверждаются в установленном порядке.

Номенклатура должностей пересматривается не реже одного раза в 5 лет.

При направлении для согласования в орган безопасности разработанной в установленном порядке номенклатуры должностей в сопроводительном письме указывается, когда и с каким органом безопасности была согласована предыдущая номенклатура должностей, какое число должностей предусматривалось в ней для оформления допуска по первой, второй и третьей формам, причины увеличения или снижения числа указанных должностей в новой номенклатуре.

Номенклатура должностей работников филиала организации (обособленного подразделения, постоянно действующей экспедиции и т.п.) перед направлением на

согласование в орган безопасности по месту нахождения филиала (подразделения, экспедиции) предварительно представляется в подразделение по защите государственной тайны вышестоящей организации.

14. При несоответствии формы допуска гражданина степени секретности сведений, к которым он фактически имеет доступ, форма допуска должна быть изменена.

Снижение формы допуска с первой на вторую (третью) или со второй на третью оформляется распоряжением руководителя организации с соответствующей отметкой в графе 8 карточки (форма 3). В случае производственной необходимости руководитель, ранее снизивший форму допуска работнику, может восстановить ее без проведения проверочных мероприятий органами безопасности.

О фактах снижения и восстановления ранее имевшейся формы допуска информируется орган безопасности.

Повышение в случае необходимости формы допуска производится в установленном настоящей Инструкцией порядке.

15. В соответствии со статьей 23 Закона Российской Федерации "О государственной тайне" допуск гражданина к государственной тайне может быть прекращен по решению руководителя организации в случае:

расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;

однократного нарушения им предусмотренных трудовым договором (контрактом) обязательств, связанных с сохранением государственной тайны;

возникновения обстоятельств, являющихся в соответствии с пунктом 5 настоящей Инструкции основанием для отказа гражданину в допуске к государственной тайне.

В случае отстранения гражданина от работы со сведениями, составляющими государственную тайну, оформляется письменное заключение, подготовленное подразделением по защите государственной тайны и структурным подразделением, в котором указанный гражданин работает. Заключение утверждается руководителем организации.

Об этом факте письменно сообщается в орган безопасности, а также делается соответствующая отметка в карточке (форма 3).

Прекращение допуска гражданина к государственной тайне является дополнительным основанием для расторжения трудового договора (контракта) с ним, если такое условие предусмотрено в этом договоре (контракте).

Решение руководителя организации о прекращении допуска гражданина к государственной тайне и расторжении на основании этого трудового договора (контракта) с ним может быть обжаловано в вышестоящую организацию или в суд.

Прекращение допуска гражданина к государственной тайне не освобождает его от взятых обязательств по неразглашению сведений, составляющих государственную тайну.

Заключение органа безопасности о нецелесообразности дальнейшего допуска гражданина к особой важности, совершенно секретным и секретным сведениям является обязательным основанием для отстранения этого гражданина от работы со сведениями, составляющими государственную тайну.

Переписка по вопросам допуска граждан к сведениям, составляющим государственную тайну, ведется в порядке, установленном для секретных документов.

Подразделение по защите государственной тайны организации ведет учет фактической степени осведомленности граждан, работающих в данной организации и допущенных к особой важности, совершенно секретным и секретным сведениям.

II. Оформление допуска

16. Подготовка материалов на граждан, оформляемых (переоформляемых) на допуск к особой важности, совершенно секретным и секретным сведениям, осуществляется управлениями (отделами) кадров, а в случае их отсутствия - работниками, ведущими

кадровую работу в организации (далее именуются - кадровый аппарат). Направлять граждан в подразделения по защите государственной тайны и органы безопасности по вопросам оформления допуска запрещается.

17. Граждане, оформляемые на допуск к государственной тайне, заполняют анкету (форма 2), в которой обязаны указывать достоверные данные.

Работники кадрового аппарата в ходе беседы с оформляемым на работу (службу) гражданином сверяют указанные в анкете данные с его личными документами (паспорт, военный билет, трудовая книжка, диплом об образовании, свидетельство о рождении и т.д.), уточняют отдельные вопросы анкеты, выявляют представляющие интерес сведения, не предусмотренные вопросами анкеты, выясняют у гражданина, имел ли он за последний год отношение к секретным работам, документам и изделиям, давал ли он обязательство по неразглашению сведений, составляющих государственную тайну, работал ли (служил) на режимных объектах, запрашивают необходимые справки и документы, знакомят гражданина с содержанием договора (контракта) об оформлении допуска к государственной тайне (форма 9).

Если в ходе беседы или в анкетных данных выявлены обстоятельства, влияющие на принятие решения о допуске гражданина к государственной тайне, или установлено, что он ранее работал с особой важности или совершенно секретными сведениями, то о результатах беседы работники
кадрового аппарата обязаны информировать в устной или письменной форме руководителя подразделения по защите государственной тайны соответствующей организации.

Заключение договора (контракта) об оформлении допуска к государственной тайне осуществляется с соблюдением всех требований гражданского и трудового законодательства Российской Федерации, а также статьи 24 Закона Российской Федерации "О государственной тайне".

Анкета оформляемого на допуск гражданина подписывается работником кадрового аппарата и заверяется печатью.

18. Подразделения по защите государственной тайны:

разрабатывают рекомендации для кадровых аппаратов по оформлению на работу граждан, подлежащих допуску;

запрашивают при необходимости из подразделений по защите государственной тайны организаций, где оформляемый гражданин в течение последнего года работал, карточку (форма 3);

дают оценку первичным материалам, представляемым кадровыми аппаратами на оформляемых (переоформляемых) граждан или получаемым из подразделений по защите государственной тайны с прежних мест работы указанных граждан, в целях определения целесообразности проведения проверочных мероприятий органами безопасности;

оформляют и хранят учетные материалы по допуску: карточки (формы 3 и 8) и списки лиц, подлежащих допуску к секретным сведениям (форма 6);

осуществляют контроль за исполнением требований по допуску.

19. На каждого гражданина, оформляемого на допуск по первой или второй форме, кадровый аппарат представляет в подразделение по защите государственной тайны, а подразделение по защите государственной тайны направляет в орган безопасности следующие документы:

а) мотивированное письмо о необходимости оформления допуска к государственной тайне. В письме указываются должность, на которую оформляется гражданин, и ее порядковый номер в утвержденной
номенклатуре должностей, количество лиц, допущенных по данной должности к сведениям, составляющим государственную тайну, номер ранее имевшегося у гражданина допуска, дата окончания проведения проверочных мероприятий и наименование органа безопасности, который их проводил (в случае переоформления допуска - причина

переоформления), отмечаются обстоятельства, влияющие на принятие решения о допуске, и дается им оценка;
б) анкета (форма 2);
в) 1 экземпляр карточки (форма 3), зарегистрированной в журнале учета карточек на допуск работников по первой и второй формам (форма 10);
г) по согласованию с органом безопасности 1 или 2 экземпляра учетной карточки на допуск по первой и второй формам (форма 5). В том случае, когда оформляемый на допуск к особой важности или совершенно секретным сведениям гражданин постоянно проживает не в месте расположения организации, а в другом регионе Российской Федерации (республика, край, область), в орган безопасности направляется дополнительный экземпляр учетной карточки (форма 5);
д) по согласованию с органом безопасности 2 или 3 экземпляра списка на оформляемого гражданина и его близких родственников (отца, мать, братьев, сестер и детей старше 16 лет), а также на жену (мужа), в том числе бывших (форма 4). При этом на каждую фамилию составляется отдельный список.
Мотивированные письма о необходимости оформления допуска к государственной тайне и карточки (формы 3 и 5) готовятся подразделением по защите государственной тайны.

20. На граждан, оформляемых на допуск по третьей форме, кадровыми аппаратами составляются общие (в алфавитном порядке) списки лиц, подлежащих допуску к секретным сведениям (форма 6), а в случаях, указанных в пункте 6 настоящей Инструкции, - списки (форма 4) по каждому лицу отдельно.

21. Карточка (форма 3) с отметкой органа безопасности о проведении проверочных мероприятий, связанных с допуском гражданина к особой важности или совершенно секретным сведениям, возвращается без сопроводительного письма и хранится в подразделении по защите государственной тайны организации вместе с договором (контрактом) об оформлении допуска к государственной тайне (форма 9) в специальной картотеке, составленной в алфавитном порядке. Такие картотеки при необходимости могут вестись по структурным подразделениям организации.
Карточка (форма 3) с момента заполнения является секретным документом и регистрируется в журнале учета карточек на допуск работников (форма 10) ответственными за их хранение лицами.
На каждого гражданина, оформляемого на допуск по первой или второй форме, заводится только одна карточка (форма 3), которая при его переходе на работу в другие организации пересылается по получении письменного запроса от соответствующего подразделения по защите государственной тайны.
Новая карточка (форма 3) заводится на работника только в случае, если ранее заведенная карточка была уничтожена по причинам, изложенным в пункте 34 настоящей Инструкции.

22. После проведения органом безопасности проверочных мероприятий решение о допуске гражданина к особой важности или совершенно секретным сведениям оформляется распоряжением руководителя организации с отметкой в графе 8 карточки (форма 3) и заверяется его подписью и печатью организации, решение о допуске к секретным сведениям - отметкой в списке лиц, подлежащих допуску к секретным сведениям (форма 6), с соответствующей записью в графе 10 карточки на допуск по третьей форме (форма 8).

23. Решение о допуске руководителей федеральных органов государственной власти и организаций федерального уровня к государственной тайне принимается лицами, которыми они были назначены на соответствующие должности.
Решение о допуске руководителей организаций, действующих в сфере ведения федеральных органов государственной власти, к государственной тайне принимается вышестоящими руководителями. В подразделения по защите государственной тайны этих организаций письменно сообщается дата окончания проведения проверочных

мероприятий, форма и номер допуска оформляемых руководителей, а также наименование органа безопасности, проводившего проверочные мероприятия. В этом случае карточки (форма 3 или 8) хранятся в подразделениях по защите государственной тайны вышестоящих организаций.

Решение о допуске к государственной тайне руководителей организаций, не находящихся в ведении федеральных органов государственной власти и впервые привлекающихся для проведения работ со сведениями, составляющими государственную тайну, принимается руководителями организаций - заказчиков работ. Карточки (форма 3 или 8) в этом случае хранятся в подразделении по защите государственной тайны организации - заказчика работ.

24. На каждое лицо, получившее допуск по третьей форме, подразделение по защите государственной тайны на основании письменного ходатайства руководителя структурного подразделения организации заводит карточку (форма 8) с указанием номера списка (форма 6) и даты утверждения руководителем организации этого списка. Заполненные карточки заверяются подписью руководителя или заместителя руководителя подразделения по защите государственной тайны и печатью этого подразделения, регистрируются в журнале учета карточек на допуск работников (форма 10) отдельно от карточек на допуск граждан по первой и второй формам и вместе со списками на лиц, подлежащих допуску к секретным сведениям (форма 6), и договорами (контрактами) об оформлении допуска к государственной тайне (форма 9) хранятся в подразделении по защите государственной тайны в течение всего периода работы в данной организации граждан, допущенных к секретным сведениям.

Карточки (форма 8) в другие организации не пересылаются и уничтожаются по истечении одного года после увольнения граждан, на которых они были заведены. При небольшом количестве граждан, оформляемых на допуск по третьей форме, карточки (форма 8) могут не заводиться.

При ведении карточного учета (форма 8) списки (форма 6) хранятся в организации в течение одного года, после чего они могут быть уничтожены в установленном порядке.

Если в соответствии с пунктом 6 настоящей Инструкции в организации допуск граждан к секретным сведениям осуществляется только после проведения проверочных мероприятий органами безопасности, то в указанные органы направляются с сопроводительным письмом 2 или 3 экземпляра списка на оформляемого гражданина (форма 4) и 1 экземпляр списка лиц, подлежащих допуску к секретным сведениям (форма 6).

О проведении проверочных мероприятий органами безопасности делается отметка в листе согласования (форма 7) или на списках (форма 6), возвращаемых в организацию вместе с сопроводительным письмом.

В этом случае входящий номер, проставляемый соответствующим органом безопасности на списке (форма 6), является и номером допуска.

25. При оформлении на работу уволенного с военной службы в запас гражданина, которому требуется допуск, кадровый аппарат организации обязан проверить наличие в военном билете специальной записи о допуске к государственной тайне в период прохождения им службы и при наличии такой записи направить запрос в военкомат по месту жительства этого гражданина для получения карточки (форма 3).

При наличии указанной записи в военном билете руководитель организации имеет право в течение одного года со дня увольнения гражданина с военной службы в запас допускать его к государственной тайне без проведения дополнительных проверочных мероприятий органами безопасности. При этом в графе 8 карточки (форма 3), полученной из военкомата, делается соответствующая запись. О факте допуска гражданина к государственной тайне информируется орган безопасности, в его адрес подразделение по защите государственной тайны соответствующей организации направляет учетную карточку (форма 5).

При оформлении на работу офицеров, прапорщиков (мичманов), уволенных в запас или в отставку и имевших допуск к государственной тайне, карточка (форма 3) запрашивается в соответствующем военкомате по месту жительства.

26. Руководители организаций, не включенных в перечень объектов, на которых допуск к секретным сведениям осуществляется только после проведения проверочных мероприятий органами безопасности, могут направлять в органы безопасности материалы на граждан, допускаемых к секретным сведениям, в случае, когда имеются обоснованные сомнения в достоверности их анкетных данных. При этом в орган безопасности направляется сопроводительное письмо с указанием обстоятельств, влияющих на принятие решения о допуске соответствующего гражданина, 3 экземпляра списка (форма 4), 1 экземпляр списка (форма 6) и другие материалы, необходимые для принятия решения по данному вопросу.

Орган безопасности дает ответ на обороте списка (форма 6), который хранится в подразделении по защите государственной тайны в соответствии с пунктом 24 настоящей Инструкции.

27. Студенты высших и средних специальных учебных заведений, достигшие 16-летнего возраста, как правило, допускаются только к секретным сведениям.

К совершенно секретным сведениям студенты высших и средних специальных учебных заведений могут быть допущены лишь в исключительных случаях, когда это обусловлено спецификой учебного процесса, подготовкой дипломных работ или прохождением практики в организациях. Оформление допусков осуществляется в соответствии с требованиями настоящей Инструкции. По окончании учебы карточка (форма 3) при наличии письменного запроса пересылается по месту дальнейшей работы выпускника.

Студенты последних курсов высших и средних специальных учебных заведений, не имеющие допуска, при распределении на постоянную работу в организации могут оформляться на допуск по первой или второй форме по месту предстоящей работы в установленном настоящей Инструкцией порядке, но не позднее чем за 3 месяца до окончания учебы. По запросам этих организаций руководители высших и средних специальных учебных заведений обязаны выслать в их адрес анкеты (форма 2) оформляемых студентов.

28. Студенты и другие лица, не достигшие 16-летнего возраста, могут быть допущены по решению руководителей организаций только к секретным сведениям.

Руководители организаций несут персональную ответственность за обеспечение режима секретности при осуществлении этими лицами своих служебных функций.

По достижении 16-летнего возраста такие лица при необходимости подлежат оформлению на допуск по второй форме в порядке, предусмотренном настоящей Инструкцией.

III. Переоформление допуска

29. Переоформление допуска граждан по первой и второй формам производится соответственно через 10 или 15 лет только в случае перехода указанных граждан на другое место работы.

Переоформление допуска граждан, постоянно работающих в организации, оформившей им допуск, не производится.

30. Переоформление допуска по первой или второй форме независимо от сроков действия производится в случае:

а) перевода или приема гражданина на работу (назначения на должность) в подразделение по защите государственной тайны, шифровальные или мобилизационные органы;

б) вступления гражданина в брак, кроме случаев, предусмотренных пунктом 31 настоящей Инструкции;

в) возвращения из длительных (свыше 6 месяцев) заграничных командировок;

г) выезда близких родственников гражданина за границу на постоянное место жительства;

д) возникновения иных обстоятельств, влияющих в соответствии с пунктом 5 настоящей Инструкции на принятие решения о допуске.

При переоформлении допуска в органы безопасности направляются документы, указанные в пункте 19 настоящей Инструкции.

31. Если вступают в брак граждане, работающие в одной организации и имеющие допуск по первой или второй форме, то переоформление допуска не производится. Если при этом гражданин изменяет фамилию, подразделение по защите государственной тайны делает соответствующую отметку в карточке (форма 3). Организация направляет в орган безопасности письменное уведомление о вступлении в брак лиц, которые имеют допуск к особой важности и совершенно секретным сведениям, и об изменении фамилии одного из них с приложением учетной карточки (форма 5).

В случае изменения фамилии гражданином, имеющим допуск к секретным сведениям, подразделение по защите государственной тайны делает соответствующую отметку в карточке (форма 8).

32. Подразделение по защите государственной тайны, получив карточку (форма 3) на гражданина с прежнего места работы, определяет необходимость переоформления ему допуска и докладывает об этом руководителю организации.

Если переоформления допуска не требуется, руководитель организации разрешает допуск гражданина, о чем делается соответствующая отметка в графе 8 карточки (форма 3), а подразделение по защите государственной тайны проводит инструктаж допускаемого лица, заключает договор (контракт) об оформлении допуска к государственной тайне (форма 9) и не позднее чем через месяц направляет в орган безопасности учетную карточку (форма 5), на обороте которой указаны форма и номер допуска, дата окончания проведения проверочных мероприятий соответствующим органом безопасности.

33. Кадровые аппараты обязаны своевременно информировать подразделения по защите государственной тайны о всех изменениях в анкетных данных граждан, допущенных к особой важности, совершенно секретным и секретным сведениям, для решения вопроса о целесообразности переоформления им допуска в соответствии с порядком, установленным настоящей Инструкцией.

При инструктаже указанных граждан подразделения по защите государственной тайны обязаны предупреждать их о необходимости своевременно информировать кадровые аппараты о всех изменениях анкетных данных.

34. В отношении граждан, которые свыше года после оформления им допуска по первой, второй или третьей форме не соприкасались со сведениями, составляющими государственную тайну, а также граждан, которые уволились из организации, ушли на пенсию или закончили обучение в учебном заведении и на которых в течение года не затребованы карточки (форма 3), действие допусков прекращается, при этом договоры (контракты) об оформлении допуска к государственной тайне (форма 9) и карточки (форма 3) хранятся в подразделении по защите государственной тайны в течение установленного срока (форма 3 - не менее 5 лет, форма 8 - 1 год), после чего карточки вместе с договорами (контрактами) уничтожаются по акту.

Прекращение действия допуска по первой и второй формам оформляется соответствующими ежеквартальными актами, составленными в произвольной форме с указанием фамилий граждан в алфавитном порядке, дат и мест их рождения. Акты утверждаются заместителем руководителя организации, занимающимся вопросами защиты государственной тайны, или руководителем подразделения по защите государственной тайны, их копии направляются в орган безопасности, осуществляющий проверочные мероприятия.

IV. Порядок доступа граждан к особой важности, совершенно секретным и секретным сведениям при командировании их в другие организации

35. Доступ граждан к особой важности, совершенно секретным и секретным сведениям

в организациях, куда они командируются по служебным делам, осуществляется после предъявления ими документов, удостоверяющих личность, справок о допуске и предписаний на выполнение заданий (форма 16).

Военнослужащим органов безопасности при командировании их в организации, не входящие в систему органов Федеральной службы безопасности Российской Федерации, предоставляется право доступа к особой важности, совершенно секретным и секретным сведениям по предъявлении предписаний на выполнение заданий (форма 16) и документов, удостоверяющих личность.

Сотрудникам органов безопасности, осуществляющим по роду службы непосредственное взаимодействие с организациями в работе по защите государственной тайны, такое право предоставляется по предъявлении удостоверения личности.

36. Гражданам, командируемым в другие организации, а также в органы военного управления, соединения, воинские части, учреждения, военные учебные заведения, на предприятия и в организации Министерства обороны Российской Федерации, органы, штабы, части и учреждения других министерств и ведомств Российской Федерации, где законодательством предусмотрена военная служба (далее именуются - воинские части), выдаются справки, удостоверяющие наличие у них соответствующего допуска:

имеющим допуск к сведениям особой важности - справка о допуске по первой форме (форма 11), в которой после буквенного индекса "А" указывается номер допуска и дата окончания проведения проверочных мероприятий органом безопасности;

имеющим допуск к совершенно секретным сведениям - справка о допуске по второй форме (форма 12), в которой после буквенного индекса "Б" указывается номер допуска и дата окончания проведения проверочных мероприятий органом безопасности;

имеющим допуск к секретным сведениям - справка о допуске по третьей форме (форма 13), в которой после буквенного индекса "Д" указывается номер распоряжения руководителя организации о допуске или списка (форма 6) и дата.

37. Справка о допуске командированного лица подписывается руководителем подразделения по защите государственной тайны или кадрового аппарата и заверяется печатью организации.

Указанная справка выдается подразделением по защите государственной тайны под расписку командированного лица в журнале учета выдачи справок о допуске (форма 14) или в карточке учета выдачи справок о допуске (форма 15) на срок разовой командировки или на срок выполнения задания, но не более чем на год, после чего она возвращается по месту ее получения и уничтожается, о чем делается отметка в журнале (форма 14) или карточке (форма 15), которая заверяется подписями двух сотрудников подразделения по защите государственной тайны. При этом акт на уничтожение не оформляется. Журнал (форма 14) и карточка (форма 15) хранятся в подразделении по защите государственной тайны не менее 5 лет после внесения в них последней записи, а затем уничтожаются в установленном порядке.

Делать в справке отметки, содержащие сведения, составляющие государственную тайну, запрещается.

38. Для посещения технических территорий режимных объектов по несекретным вопросам командированному лицу необходимо иметь справку о допуске по третьей форме (за исключением случаев, предусмотренных настоящей Инструкцией).

39. Требовать от командированного лица, прибывающего в организацию для выполнения задания секретного или несекретного характера, представления справки о допуске к особой важности или совершенно секретным сведениям запрещается. Исключение составляет случай, когда указанное лицо при выполнении задания неизбежно будет иметь доступ к особой важности или совершенно секретным сведениям.

Руководитель организации и подразделение по защите государственной тайны должны принимать все необходимые меры к созданию таких условий для приема указанной категории командированных граждан, при которых исключалась бы возможность их

ознакомления с особой важности или совершенно секретными сведениями.

40. Предписание на выполнение задания (форма 16) подписывается руководителем организации или руководителем структурного подразделения организации, а в министерствах и ведомствах - начальником главного управления, управления или самостоятельного отдела. Предписание заверяется печатью организации или печатью подразделения по защите государственной тайны. В предписании кратко указывается основание командирования (номер и дата постановления, решения, договора, совместного плана научно-исследовательских и опытно-конструкторских работ и т.п.), а также определяется, с какими сведениями, составляющими государственную тайну, необходимо ознакомить командируемое лицо для выполнения им задания.

Предписание, в котором содержатся особой важности, совершенно секретные или секретные сведения, пересылается почтой в порядке, установленном для секретных документов.

Предписание выдается для посещения только одной организации.

41. Командированное лицо может иметь доступ только к тем особой важности, совершенно секретным и секретным сведениям, которые ему необходимы в рамках выполняемого задания, указанного в предписании на выполнение задания (форма 16). Доступ осуществляется с письменного разрешения руководителя принимающей организации, а в министерствах и ведомствах - начальника главного управления, управления или самостоятельного отдела (для ознакомления со сведениями особой важности) либо руководителя структурного подразделения (для ознакомления с совершенно секретными и секретными сведениями).

В отдельных случаях, определяемых руководителями министерств и ведомств или заказчиками работ, командированные лица могут иметь доступ к особой важности, совершенно секретным и секретным сведениям в принимающих организациях только с их письменного разрешения.

42. Предписание на выполнение задания (форма 16) с разрешением соответствующего руководителя ознакомить командированное лицо с особой важности, совершенно секретными или секретными сведениями вместе со справками о допуске регистрируются подразделением по защите государственной тайны в журнале учета командированных (форма 17). После регистрации справка о допуске остается в подразделении по защите государственной тайны, а предписание на выполнение задания с визой соответствующего руководителя и отметкой о форме допуска командированного лица передается принимающим его должностным лицам. Указанные должностные лица производят на обороте предписания отметки о степени секретности сведений, с которыми фактически ознакомилось командированное лицо. Отметки подтверждаются подписью командированного лица, после чего предписание передается для хранения в подразделение по защите государственной тайны, а справка о допуске возвращается ее владельцу для сдачи в подразделение по защите государственной тайны по месту его постоянной работы. Предписание хранится в специальном деле в подразделении по защите государственной тайны не менее 5 лет.

На обороте справки о допуске (форма 11 или 12) указываются степень секретности сведений, с которыми ознакомилось командированное лицо, и дата. Запись заверяется подписью руководителя подразделения по защите государственной тайны и печатью указанного подразделения.

Работникам органов и учреждений прокуратуры Российской Федерации достаточно иметь предписания на выполнение заданий и удостоверения личности с отметкой о допуске к государственной тайне.

Военнослужащим достаточно иметь предписания на выполнение заданий и удостоверения личности (военные билеты) с отметкой о допуске к государственной тайне, заверенной гербовой печатью, при условии их командирования в воинские части, находящиеся в подчинении министерства или ведомства, в котором указанные

военнослужащие проходят военную службу.

43. Студенты и аспиранты высших учебных заведений и студенты средних специальных учебных заведений для прохождения производственной практики могут быть допущены, как правило, на те режимные объекты, которые выделены в установленном порядке конкретным учебным заведениям на определенный период в качестве баз для прохождения практики по соответствующим специальностям.

Организации, занятые разработкой, проектированием, изготовлением и испытанием опытных и серийных образцов новейших видов вооружения и оборонной техники, не могут быть закреплены в качестве баз для прохождения практики студентами. Студенты могут быть допущены в указанные организации, а также в другие организации, не выделенные в качестве баз для прохождения практики, только на преддипломную практику в случае, если они за год до окончания учебного заведения распределены на постоянную работу в эти организации. При прохождении практики на режимных объектах студенты допускаются к совершенно секретным и секретным сведениям с разрешения руководителей структурных подразделений, которые совместно с подразделениями по защите государственной тайны определяют характер и объем совершенно секретных и секретных сведений, с которыми студенты могут быть ознакомлены или которые могут быть ими использованы в дипломных работах.

44. Граждане, работающие над диссертациями (монографиями и т.п.), допускаются к носителям особой важности, совершенно секретных или секретных сведений, находящимся на хранении в государственных архивах, по предъявлении справок о допуске (форма 11, 12 или 13) и предписаний (форма 16) и с разрешения организации, формирующей фонд архивного хранения, либо ее правопреемника в порядке, утверждаемом Государственной архивной службой России.

45. Члены экипажей судов загранплавания при командировании их на режимные объекты для приемки и ремонта судов могут проходить на эти объекты по судовой роли с предъявлением паспорта моряка.

В этом случае подразделение по защите государственной тайны обязано проинструктировать их о правилах режима секретности в данной организации.

46. Специально назначенные представители государственных надзорных органов, финансовых и налоговых органов, органов налоговой полиции, энергосбыта и других органов, непосредственно связанных с обслуживанием режимных объектов, могут посещать указанные объекты только при наличии справок о допуске (форма 11, 12 или 13), соответствующих степени секретности выполняемых работ.

В таком же порядке на указанных объектах осуществляется доступ к государственной тайне работников органов внутренних дел и других правоохранительных органов.

47. Надзор за соблюдением законодательства Российской Федерации при обеспечении защиты государственной тайны и законностью принимаемых при этом решений осуществляет Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Доступ лиц, осуществляющих прокурорский надзор, к государственной тайне обеспечивается в порядке, предусмотренном настоящей Инструкцией.

48. Лица, виновные в нарушении требований настоящей Инструкции, несут ответственность в соответствии с действующим законодательством.

49. Порядок допуска граждан к государственной тайне в условиях объявленного чрезвычайного положения может быть изменен Президентом Российской Федерации.

Рекомендуемая литература

1. Закон Российской Федерации "О государственной тайне"

2. Постановление Правительства РФ от 28 октября 1995 г. N 1050 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к

государственной тайне"
3. Перечень медицинских противопоказаний для осуществления работы с использованием сведений, составляющих государственную тайну, утвержден приказом Минздрава РФ от 16 марта 1999 г. N 83
4. Общие положения Инструкции "о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
5. Постановление Правительства РФ от 22 августа 1998 г. N 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне"
6. Копылов В.А. Информационное право: Учебное пособие. - М.: Юристъ, 2013. - 472 с.
7. Рассолов М.М. Информационное право: Учебное пособие. - М.: Юристъ, 2014. - 400 с.
8. Горбатов В.С., Кондратьева Т.А. Информационная безопасность. Основы правовой защиты: Учебное пособие. М.: МИФИ, 2021.
9. Организация и современные методы защиты информации/Под общ. Ред. Диева С.А., Шаваева А.Г. М.: Концерн "Банковский деловой центр", 2014. - 472 с.

Лабораторное занятие №4.

Тема: Использование специальных психологических методик, уникальных психофизических методов и компьютерных психотехнологий при подборе персонала на работу с конфиденциальной информацией.

СОДЕРЖАНИЕ ЗАНЯТИЯ

Введение

Известно, что 51.7 % угроз предпринимательской деятельности совершается либо самими сотрудниками фирмы либо при их прямом или опосредованном участии. Следовательно безопасность коммерческой деятельности в значительной мере зависит от того, в какой степени квалификация ее сотрудников, их морально-нравственного качества соответствуют современным требованиям. Существующая на сегодня практика подбора кадров опирается прежде всего на выяснение уровня профессиональной подготовки кандидатов на работу, который определяется по традиционно-формальным признакам; образование, стаж работы. Ныне требования к сотрудникам коммерческих фирм существенно повышаются и расширяются. Это обстоятельства побуждает руководителей фирм значительно усилить требования к подбору, расстановке и воспитанию кадров, к использованию методов и процедур научной психологии, с помощью которых можно достаточно быстро, надежно и всесторонне оценивать возможности каждого сотрудника и составлять его психологический портрет.

С точки зрения экономической безопасности такой профессиональный отбор кандидатов и сотрудников обеспечивает:

- выявление ранее имевших место судимостей, преступных связей, криминальных наклонностей
- определение предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков при определенных обстоятельствах
- установление фактов морально-психологической ненадежности, неустойчивости, уязвимости, мнительности и др.

Как правило, проблема отбора кадров встает перед руководителем фирмы в следующих случаях: подбор кадров при формировании штатов, замещение вакантных должностей.

Для первого случая характерно изучение значительного числа кандидатов, для которых из набора имеющихся штатных должностей подбирается соответствующая. Во втором случае из ограниченного числа кандидатов отбирается тот, который по своим личным и профессиональным качеством в наибольшей степени соответствует требованиям данного рабочего места.

Как в том, так и в другом случае профотбор персонала реализуется по следующей схеме:

1. Предварительное собеседование
2. Сбор и оценка сведений о кандидате
3. Тестовые процедуры проверки кандидата
4. Анализ результатов проверки и тестирования
5. Заключительное собеседование

При подборе сотрудников на работу могут использоваться специальные психологические методики, уникальные психофизические методы и компьютерные психотехнологии. Проверяется профессионализм кандидатов на ту или иную должность, их надежность и лояльность интересам фирмы, скрытые мотивы поведения и так далее.

Вопрос 1. Метапрограммы в подборе и оценке персонала

Профессиональные рекрутеры или специалисты отдела HR часто сталкиваются с такой задачей: необходимо подобрать специалиста на рабочую вакансию, а претендентов несколько. И все очень приятные в общении люди, грамотно отвечающие на поставленные вопросы. По каким критериям выбрать из них подходящего?

Профессионалы, давно работающие в этой области, делают это легко и именуют свое мастерство интуицией. Но практически не могут передать свой опыт другим, так как его

трудно формализовать. Начинающие же работу в этой области нарабатывают свой собственный опыт ценой проб и ошибок, часто приводящих к потерям собственного рабочего времени и лишним материальным затратам компании.

Итак, нужны система, структура построения интервью, четко разработанные критерии, простая и универсальная технология, которая обобщит и структурирует опыт. И нужен язык описания.

Хорошая новость заключается в том, что вся эта система уже существует. Она не противоречит действующим тестам и методикам, а легко интегрируется с ними. Кроме того, вы «встраиваете в себя» все необходимые тесты. Для ее освоения не обязательно быть психологом — вы становитесь психологом «по жизни». Система достаточно универсальна, чтобы использовать ее для разных

задач — от создания модели компетенций, проведения структурированного диагностического интервью до оценки и мотивирования персонала, подбора команд и создания кадрового резерва. Эта система основана на теории метапрограмм человека.

Метапрограммы — это внутренние характеристики, способы мышления человека, на основании которых строится его поведение. Как человек мыслит, так он и действует. Если человек уверен в себе, в том, что мир вокруг него безопасен, то вы всегда заметите это в его поведении — скажем, в развороте плеч, наклоне головы — и даже говорить он будет особым образом. Если человек не уверен в себе, его беспокоят сомнения, то вы почувствуете это и в позе, и в речи. Мышление и поведение взаимосвязаны.

Метапрограммы выражаются не только в поведении, но и в речевых оборотах. Исследования в области психолингвистики (Ноам Хомский) показывают, что язык, как и внешнее поведение, отражает наше сознание. Но в обыденном общении мы часто обращаем внимание лишь на содержательную часть речи. Если мы будем обращать внимание на «форму» построения речи, то очень многое сможем узнать о человеке, ее произносящем.

Слушая, как говорит человек, наблюдая за его поведением (позы, мимика, скорость реакции, движения глаз и др.), мы можем определить его личностные особенности, которые, как правило, связаны и с профессиональными предпочтениями. Только слушать, слышать и наблюдать нужно особенным образом.

На чем строится подход?

1. Избирательность внимания. Ценности.

Я живу на длинной, насыщенной магазинами улице и всегда знаю, куда и как мне идти, чтобы быстрее купить продукты, вещи, подарки, заплатить за коммунальные услуги, что-то отремонтировать… В памяти хранится все то, что представляет определенную ценность в контексте ведения домашнего хозяйства. Но однажды, когда меня спросили, где на этой улице продаются автозапчасти,

я задумалась — не представляющая интереса (машиной я пока не занимаюсь) информация в памяти не хранилась. Потом, заинтересовавшись, на расстоянии четырех автобусных остановок я обнаружила три магазина, где были представлены всевозможные автодетали. Так устроено наше внимание — оно выбирает то, что ценно и полезно для человека в данном контексте.

Как это связано с приемом на работу? Задавая определенные вопросы, вы можете выявить зоны интересов претендентов на данную должность. Например, вы задаете вопрос трем претендентам «Что вам важно в вашей работе?» А они вам отвечают: первый — «Мне важно, чтобы я мог приносить стабильную прибыль себе и фирме»; второй — «Мне хотелось бы реализовать знания, полученные в институте…», а третий — «Ну чтоб интересно было, чтобы коллектив был хороший…» Вслушиваясь в эти слова, вы понимаете, кто из них пришел за финансовым результатом, а кто — за самореализацией, развитием или общением…

Умение работать с чужими ценностями, учитывать их, присоединяться к ним

— основа любой успешной коммуникации. Все успешные коммуникаторы, будь то

управленцы, продавцы или специалисты по связям с общественностью, обладают высокой чуткостью и гибкостью в отношении ценностей своих сотрудников, клиентов или партнеров.

2. Человек бессознательно использует в речи и поведении привычные способы мышления.

Мы привыкли думать, что в бессознательном состоянии находимся, когда спим или медитируем. На самом деле мы многое делаем бессознательно. Например, «что» говорить — еще контролируем сознательно, а вот «как» — это больше бессознательный процесс. Человек в речи обычно проявляет свой привычный способ мышления, ценности, личные особенности, которые полезно учитывать при профессиональном отборе.

3. Существует несколько основных метапрограмм, с помощью которых мозг отдельного человека организует работу с входящей и исходящей информацией.

Метапрограммы удобнее рассматривать с помощью шкал с двумя полюсами. При собеседовании обычно используется от 7 до 12 таких шкал. Рассмотрим некоторые из них.

Активность — рефлективность

Всем памятна ситуация, когда на вопрос учителя быстро поднимаются руки — это самые активные ученики сигнализируют о готовности отвечать. Не всегда, правда, ответы бывают правильными. Но таковы уж ученики активные — они сначала действуют, а только потом думают. Люди (и не только дети) активного типа предпочитают действия размышлениям. Едва задача поставлена, они срываются с места и начинают ее выполнять. «Огонь в глазах»

— это про них. Их отличает неутомимость и неусидчивость. Скорость реакции на внешние стимулы у них очень высока. Такие люди, как правило, работают за четверых. Люди рефлективного типа предпочитают сначала размышлять, потом действовать. Они словно бы экономят энергию.

И как же нам по собеседованию определить активного и рефлективного? Задайте вопрос, например: «Чем вы занимались на своей предыдущей работе?» Проследите за построением предложения — в речи активного вы услышите: «Работал с клиентами, подписывал договоры, ездил на переговоры, следил за ассортиментом продукции в магазинах...» Рефлективный же скажет вам: «Вы знаете, в моей работе было очень важно постоянно сопоставлять ситуацию на рынке и учитывать эти изменения в отношениях с нашими клиентами, с которыми у нас постоянные контакты, потому что если бы мы не учитывали этих факторов…» Наблюдения показывают: чем короче предложения, тем активнее личность. Большое количество придаточных предложений свидетельствует о рефлективности.

Представим эту метапрограмму в виде шкалы:

Крайние значения (активный «мотор» или рефлективный «тормоз») встречаются довольно редко. Но предпочтения определить все-таки можно. Статистики подсчитали, что граждан рефлективного типа раз в пять больше, чем активного. А в нашей стране — раз в шесть. Это связано с историческими особенностями, например, во времена сталинских репрессий условием выживания становилось такое личное качество людей, как рефлективность: «не высовывайся» (запрет активности) — было условием выживания, и оно передалось следующим поколениям. Времена изменились — нужны активные, смелые, предприимчивые. Но память поколений жива, активных — не так много.

Принадлежность к тому или другому типу ничего не говорит об эффективности специалиста, о качестве его работы. Хороших результатов в равной степени может достигать и активный, и рефлективный. Другой вопрос

— на каких должностях: туда, где нужно быстро действовать по ситуации (например торговый представитель, тренер, руководитель), полезно набирать активных. А в работе финансового аналитика, бухгалтера, эксперта лучше не торопиться — здесь как раз подойдут рефлективные сотрудники.

Рассмотрим еще некоторые метапрограммы.

Референция внутренняя — референция внешняя

Эта пара метапрограмм имеет отношение к тому, кто принимает решение в жизни человека и кто оценивает — сам человек, его воля или обстоятельства и другие люди.

Спросите пришедшего на собеседование: «Когда вы решали для себя, поменять работу или нет,— что на вас влияло, как вы принимали решение?» Одни ответят, что на решение повлияли другие люди: «Мой муж считает, что если я не пойду работать, то потеряю квалификацию…» или обстоятельства:

«Ситуация в стране заставила меня искать новую работу…» Это — внешнереферентные. Внутреннереферентный скажет: «Я проанализировал ситуацию, взвесил все обстоятельства и принял решение о новой работе».

Внешнереферентные постоянно нуждаются в поддержке и внешней оценке; внутреннереферентные имеют свой собственный «волевой центр», который принимает решения и берет ответственность. Задайте вопрос: «Как вы поймете

— хорошо или плохо выполнена ваша работа?» Внутреннереферентный скажет: «Если все хорошо, у меня есть внутреннее чувство удовлетворения». Внешнереферентный сошлется: «Если начальник принял отчет, если от клиентов не поступило ни одной жалобы — значит, я работаю хорошо».

Внутреннереферентные хороши на руководящих должностях, на проектах, связанных с ответственностью. Специалисты «внешнереферентные» (оценка:

«руководитель сказал» или «клиенты довольны», или «сотрудники уважают»),

напротив, подходят для исполнительских должностей. Конечно, сделать точное заключение о годности человека для работы можно, только имея метапрограммный профиль конкретной вакансии и конкретного кандидата.

Есть еще люди, ориентированные на контекст. Это также внешняя референция, но она связана не с людьми, а с обстоятельствами: человек сошлется на отчеты, нормы, графики, сроки и т.п. Опыт показывает, что хорошие топ-менеджеры второго уровня и специалисты, работающие с финансами, довольно часто узнают о том, как они поработали, глядя на цифры.

Мотивация избегания — мотивация достижения

У каждого человека есть в жизни цели. И есть внутреннее «топливо» — мотивация — энергия, необходимая для достижения цели. Предположим, два сотрудника одной организации хотят купить машину. Один хочет купить машину, чтобы иметь возможность путешествовать, иметь свободу передвижения, а другой —чтобы не ездить в час пик в метро и не таскать тяжелые грузы на себе. Цель одинаковая — покупка машины. А направление мотивации разное. У одного — на достижение удовольствия

и выгод, а у другого — на избегание дискомфорта.

Так как человеческое поведение достаточно шаблонно, можно предположить, что первому бесполезно будет объяснять, что случится, если он не выполнит ежемесячный план работы, а второго, наоборот, бессмысленно завлекать перспективами развития будущего компании. Если говорить о системах оплаты труда, то те, что включают только штрафы, рассчитаны на людей с мотивацией избегания и не будут работать по отношению к тем, у кого мотивация достижения. Системы, включающие только поощрения, окажутся малоэффективными для тех, у кого мотивация избегания. Хотя дело не столько

в системе, сколько в том, как ее использовать с конкретными людьми. Одному стоит сказать: «Работай хорошо — получишь премию». А другому: «Смотри, будешь работать плохо — премии лишим!»

Направление внимания на себя — на других

Эта пара метапрограмм формируется вокруг вопроса: чьи интересы — свои собственные или интересы других людей являются для человека более важными.

Есть люди, которые и позой, и голосом, и всеми мыслями выражают внимание к собеседнику. Когда они говорят, вы понимаете, что они говорят для вас. Когда слушают, вам понятно, что они действительно вас слушают. Они делают это естественно, и вам еще

и еще раз хочется зайти к этому продавцу или агенту. Это то качество, которое мы называем «клиентоориентированность». А есть другие люди, разговаривая с которыми чувствуешь отстраненность и холодность, их внимание направлено целиком на себя. Понять, что они вообще вас слушают, очень трудно. Специалистов с направлением внимания «на себя» не назовешь клиентоориентированными!

Как вы думаете, в каких профессиях полезно набирать сотрудников с вниманием «на других»? Конечно же, это продавец в торговом зале или человек, который работает с рекламациями и жалобами покупателей. А вот налоговому инспектору или контролеру на транспорте вряд ли полезно быть

«клиентоориентированным» — не соберут они налоги и штрафы, если будут сочувственно выслушивать должников…

Итак, в нашем подходе люди не рассматриваются как хорошие или плохие, каждое рабочее место уникально и требует соответствующего специалиста. Метапрограммный подход дает возможность соизмерить личные качества

человека и качественные требования должности, что делает его удобным инструментом для составления модели компетенций, подбора и оценки персонала компании или команды, построения кадрового резерва, написания должностных инструкций. Понимание и учет особенностей и ценностей человека позволяют более точно мотивировать его к работе. Это важно в работе менеджера по персоналу или любого руководителя.

Вопрос 2. Обзор методик, применяющаяся в корпоративной практике тестирования персонала

Тесты и личностные опросники не теряют своей популярности в России.

Полный абстракционизм

Нарисовал лошадь. По крайней мере, это существо было больше всего похоже именно на нее. Однако шея у нее была слишком длинная, а хвост висел мочалой, вместо того, чтобы торчать кверху или хотя бы развеваться параллельно земле. «Это означает, что у вас заниженная самооценка, а эмоции часто выходят из под контроля»,– проинтерпретировала Анна Мостяева, ведущий психолог компании АКМР. Ну все, на позиции, где нужна уравновешенность и напористость (например, директор по продажам), уже точно не попасть.

Эту картинку помнят многие. Не одна тысяча кандидатов рисовала чудищ под наблюдением рекрутера или HR-специалиста компании. «Большинство HR- ов,– рассказывает Вероника Ярных, кадровый консультант консалтинговой группы СЭТ,– выбирают те тестовые методики или личностные опросники, которые им нравятся. Те, в которых разбираются хорошо. Например, знает человек тест Люшера (см. СФ 09/2003) – и применяет его во всех случаях, практически где ни попадя». И РНЖ («рисунок неизвестного животного» – та самая лошадь) из-за своей простоты, малых временных затрат и легкости интерпретации пользуется огромным спросом у большинства специалистов по управлению персоналом. Естественно, применять его можно только, когда есть желание дополнить впечатление о кандидате – ни о какой абсолютной валидности здесь и речи быть не может. Например, сейчас я тоже умею рисовать невиданных зверей – причем правильно.

А вот правильное применение тестов и опросников в российской корпоративной практике встречается редко. Хорошо, если тесты внедряют под заказ специализированные компании. Однако чаще руководство просто доверяется предпочтениям своих HR-ов.

Тестовый беспредел

Многие отечественные корпорации сегодня открывают для себя технологии тестирования заново. После ажиотажного бума начала 1990-х годов, когда в страну стали массово привозить нелицензированные, а, вернее, краденые западные тесты, HR-ы столь же массово от них отказывались. Слишком много подделок, а значит, бесполезных результатов. Слишком много денег тратилось впустую.

Сейчас тесты отвоевывают позиции. Иногда этому способствуют экономические

соображения. «Надо понимать, что тесты и опросники помогают сэкономить массу денег и снизить риски при подборе персонала – как и все стандартизированные продукты»,– говорит Ирина Бевз. Иногда – необходимость унификации стандартов. Ирина Горбачева, начальник отдела оценки, обучения и развития персонала ОАО «Ростелеком»: «Тестирование в нашей компании, крупной и с территориально удаленными филиалами, позволяет охватить оценкой одновременно большое количество сотрудников из разных регионов». И часто тесты выбирают просто потому, что «надо же что-то такое делать».

Тип на тип не приходится

В России две школы тестирования – отечественная и иностранная. Основа первой – когорта выпускников факультета психологии МГУ. Принципы другой привнесли сюда «импортные» компании вроде SHL – крупнейшего провайдера продуктов такого рода в России. Иностранцы изначально ориентировали все программы и линейки продуктов на нужды бизнеса, подобрали соответствующие батареи тестов и работают под заказ. Российские же компании конкурентами они не считают: «Конечно, мы не можем сказать, что у нас больше мозгов, чем у тех, кто закончил МГУ,– говорит Том Роулинз, управляющий директор компании SHL в России. Потом довольно ухмыляется и продолжает.– Да вот только играют они на несколько другом поле. Их тесты и опросники больше годятся для оценки, при которой не важны бизнес- способности – например, при психодиагностике, выявлении отклонений».

Как и положено представителю российской школы, генеральный директор HR-лаборатории «Гуманитарные технологии» Алексей Серебряков заканчивал факультет психологии МГУ. Однако причисление к «клинике» его возмущает:

«Российские разработки бизнес-тестов ничем не уступают западным. Просто у западных методик "упаковка" ярче. Да и не всегда они адаптированы к российским условиям должным образом».

В соответствии с дилеммой «бизнес-практика – клиника» используемые компаниями тесты можно разделить на две группы – функциональные (тесты достижений, бизнес-тесты) и психологические. Первые специфичны для какой-либо отрасли либо профессии (например, тесты для бухгалтеров, программистов и т. п.). Иногда такие тесты и опросники разрабатываются самими корпорациями, однако возможно и сотрудничество с провайдерами или простая покупка – например, теста для бухгалтеров.

С психологическими тестами и опросниками все запутаннее – брэндированных методик на рынке очень много. Другое дело, что получить информацию о том, в каких компаниях какие технологии применяются, очень сложно.

Переходя на личности

Психологические тесты – самая многочисленная и самая разношерстная группа методик, применяющаяся в корпоративной практике тестирования персонала. Условно их можно разделить на несколько групп:

1. Интеллектуальные. – наиболее известны непосвященным. Знаменитый тест на IQ Айзенка – из этой плеяды. По идее, такие методики должны выявлять уровень интеллектуального развития человека. Однако в кадровом менеджменте практически бесполезны, так как не адаптированы к российским условиям и – кроме того – не дают представления об истинном уровне умственного развития.
2. Социально-психологические. Дают представление о социальной компетентности человека – конфликтности-неконфликтности, его ролевых качествах в группе. Например, склонных к соперничеству или, напротив, стремящихся к компромиссам. Эти тесты также помогают оценить степень адаптации каждого члена коллектива к совместной деятельности. Распространены достаточно широко.
3. Личностные. В этой группе – знаменитый опросник MMPI (Minnesota Multiphasic Personality Inventory), который HR-специалисты обычно вспоминают первым. Дают представление об индивидуально-психологических особенностях личности, типичных

способах поведения человека. В бизнес-практике применяются, несмотря на то, что их, часто называют «клиникой». К ним также обычно относят проективные методики – самые популярные в среде российского HR. Что может быть проще, чем заставить кандидата нарисовать что-либо («Рисунок неизвестного животного») или рассказать об ассоциациях, возникающих при взгляде на некие абстрактные картины (ТАТ – тематический апперцептивный тест).

4. Тесты способностей. В компании SHL, например, из всех тестовых методик только их и признают. Пользуются стабильной популярностью, так как позволяют определить уровень развития качеств, необходимых кандидату для занятия определенной должности. Например, внимания и памяти. Иногда к этой группе относят и весьма популярный в России КОТ (краткий ориентировочный тест).

Шорт-лист самых популярных методик.

Отечественные компании предпочитают не покупать лицензий на западные тесты и опросники – даже самые популярные. А контрафактные продукты применяют почти все. Неудивительно, что говорить об этом не хотят. Единственный достоверный источник информации в этом случае – приватные беседы со знакомыми HR-ами и консультантами.

Если компания не хочет пользоваться нелицензионным продуктом, у нее есть два выхода – купить тест у разработчика или разработать самим. Но разработка собственного психологического теста (в отличие от профессионального) – дело трудоемкое и доступно лишь крупным и состоятельным компаниям, которые обычно тоже привлекают к этой работе провайдера.

Поэтому, можно считать, повезло транснациональным корпорациям, приходящим в Россию с арсеналом собственных тестовых методик и опросников. Так, у компании Procter & Gamble на одном из этапов отбора применяется так называемый Problem Solving Test (PST), который разработан сотрудниками компании P&G приблизительно 10 лет назад и с тех пор периодически обновляется. Этот тест является стандартным рекрутинговым инструментом компании и используется практически во всех странах, где работает P&G.

Великолепное разнообразие

Сегодня круг «тестовых» предпочтений российского кадрового менеджмента формируют несколько факторов – необходимость делать выбор между лицензионными и контрафактными продуктами, вялотекущая борьба двух школ – российской и иностранной. А также быстрые темпы роста компаний, из-за чего зачастую используется то, что проще освоить и быстрее внедрить. В результате лицо рынка меняется. Какие-то продукты набирают популярность. Какие-то (вроде теста Айзенка) в профессиональной среде уже практически забыты. Опросив HR-специалистов в компаниях, а также почитав крики о помощи на форумах кадровых сообществ, мы сформировали десятку самых популярных кадровых методик.

Нетрудно догадаться, что по частотности применения в практике российского HR-менеджмента впереди всех проективные методики. Освоить их несложно. Правда, и информации с их помощью много не получишь. Тем не менее базовые представления о личности все же дают. Итак, лидер рейтинга всем надоевшие «Рисунок неизвестного животного» и «Дом, дерево, человек».

1. Немного отстает по популярности от проективных методик, но также практически вне конкуренции – КОТ. Как заметил руководитель отдела обучения персонала одной из крупнейших российских корпораций: «Недавно мы начали проект по использованию краткого ориентировочного теста для подбора рабочих. До этого надобности в тестировании вообще не испытывали. А КОТ выбрали за простоту и за то, что его автор нам был неизвестен – о лицензии можно было не беспокоиться». Тест находится «на пограничье» интеллектуальных методик и тестов способностей. Позволяет оценить скорость и логику мышления, внимательность, получить представление о базовом уровне развития интеллекта. Главный недостаток – примитивность: применять КОТ можно

только при наборе персонала самого низкого звена.

2. Тест Майерс Бриггс (Myers Briggs Type Indicator). Одна из самых интересных методик, не теряющая своей популярности уже несколько лет. Основана на идеях Юнга. Включает четыре шкалы, которые являются индикаторами базисных предпочтений человека (экстраверсия – интроверсия; сенсорность – интуиция; мышление – чувствование; решение – восприятие). Комбинация личностных предпочтений составляет индивидуальный профиль человека. С его помощью можно определить, какая модель поведения человеку ближе: «коммуникатор», «стабилизатор», «стратег» или «пожарник». «Как-то раз мы тестировали одну региональную компанию по Майерс Бриггс,– рассказывает Вероника Ярных.– Выяснилось, что в компании лучше и дольше всего работают люди определенного типа – "стратеги". "Пожарники" там вообще не задерживались. Сейчас руководство решило, что при приеме на работу первым делом надо давать тест Майерс Бриггс. Если человек оказывается "пожарником" – до свиданья. Человек с таким личностным профилем в атмосферу компании, скорее всего, не впишется».

3. Группа тестов способностей (таблицы Шульте, тест Бурдона, методика Мюнстерберга и др.). Позволяют определять, насколько у кандидата развита память, внимание, способность к анализу. Просты и потому популярны.

4. Опросник Томаса. Включает 30 вопросов, позволяет выделить типичные способы реагирования сотрудников на конфликтные ситуации (сотрудничество, компромисс, уступчивость, избегание, доминирование). По словам Анны Мостяевой, «может с успехом применяться и при исследовании возможного стиля ведения переговоров и аспектов взаимодействия с клиентами». Идеальный случай – оценка кандидатов на позиции менеджера по продажам. Кадровый голод в этом сегменте рынка труда – причина того, что популярность этой методики растет взрывообразно.

5. Опросник Кеттелла. Позволяет проводить психодиагностические исследования личности, включает задания на диагностику уровня интеллектуального развития. В отличие от опросника Томаса быстро теряет популярность. Как отмечает Анна Мостяева, «все вопросы в нем "лобовые", слишком легко "читаются"». В России часто применяется аналогичная многофакторная методика Александра Шмелева.

6. Тест Люшера. Многие HR-ы только его и применяют. В основном из-за простоты, отчасти – из-за «раскрученности». Позволяет по цветовым предпочтениям определять эмоциональное состояние, мотивационную сферу, а также особенности взаимоотношений с другими людьми.

7. Опросник уровня субъективного контроля (УСК). Предназначен для того, чтобы определить, в какой степени человек готов брать на себя ответственность за то, что происходит с ним и вокруг него. Один из самых популярных методов оценки персонала при создании внутреннего резерва и составлении плана карьерного продвижения.

8. MMPI. Его знают все, а вот применяют уже немногие. Пик его популярности пройден. MMPI слишком громоздок (более 500 вопросов) и «клиничен». Выявляет черты и типы характера, стиль поведения и общения, способность к адаптации и скрытые психические отклонения, в некоторой степени помогает оценить профессиональную пригодность кандидата или сотрудника. В России есть адаптированный вариант этого теста – СМИЛ (редакция Л. Собчик), который не менее объемен (полный вариант содержит 566 вопросов, а сокращенный – 366). В результате обработки данных этого опросника получается так называемый профиль – числовое выражение оценочных шкал, используемых при расшифровке теста. Именно профиль характеризует особенности личности и психическое состояние испытуемого.

9. Особняком стоят продукты SHL. Тесты способностей и опросники этой компании пользуются спросом у потребителей, предпочитающих покупать лицензионные продукты. Среди опросников наиболее известны OPQ (профессиональный личностный опросник) и

MQ (мотивационный опросник). Самые популярные батареи тестов – AMT (тесты для руководителей высшего звена), CRTB (анализ информации), MGIB (тесты для менеджеров).
На 90 вопросов OPQ (профессиональный личностный опросник, продукт компании SHL) в среднем отвечают 40–50 минут.

Рекомендуемая литература

1. Копылов В.А. Информационное право: Учебное пособие. - М.: Юристъ, 2021. - 472 с.
2. Рассолов М.М. Информационное право: Учебное пособие. - М.: Юристъ, 2014. - 400 с.
3. Горбатов В.С., Кондратьева Т.А. Информационная безопасность. Основы правовой защиты: Учебное пособие. М.: МИФИ, 2021.
4. Организация и современные методы защиты информации/Под общ. Ред. Диева С.А., Шаваева А.Г. М.: Концерн "Банковский деловой центр", 2013. - 472 с.
5. Метапрограммы в подборе и оценке персонала Автор: Ирина Мягкова Источник: Персонал-микс 3(22)2014
6. Тест для тестов. Автор: Андрей Вырковский Источник: Секрет Фирмы, 2014г.

Лабораторное занятие №5.
Тема: Юридические меры охраны конфиденциальных сведений как составная часть корпоративной системы защиты информации.

СОДЕРЖАНИЕ ЗАНЯТИЯ
Введение

Нынешний век, наверно, уже войдет в историю человечества как век информации, и роль информации в жизни цивилизации все возрастает. Информация сегодня – это и средство обеспечения успеха в бизнесе, и объект самой серьезной защиты, это и один из наиболее значимых активов предприятия, и один из наиболее существенных элементов предпринимательских рисков. К сожалению, информационные системы становятся все более уязвимыми, требующими серьезной многоуровневой защиты, механизмов контроля и резервирования. Существенно вырастает цена, которую приходится платить владельцу ценной информации, не предпринимающему к защите своих тайн должных усилий.
Рассмотрим ситуацию, которая может сложиться в любой компании. Начальник отдела обратился в техническую службу с просьбой посмотреть электронную переписку с клиентом, которую вел один из сотрудников его отдела. Причиной обращения стала производственная необходимость:
сотрудник находится в отпуске, а ответить клиенту надо срочно. Специалист службы технической поддержки предоставил начальнику отдела доступ к корпоративному почтовому ящику «отпускника», начальник просматривает переписку в поисках нужного письма от клиента и вдруг видит сообщения, из которых узнает, что его подчиненный регулярно передает своему другу конфиденциальные сведения о компании. Более того, фирма, где работает тот друг, является конкурентом. Начальник сообщает о факте обнаружения
«коммерческого шпионажа» руководству компании, и вернувшегося из отпуска сотрудника ждет трудовая книжка с указанием следующей причины увольнения: п.в) ч.6 ст.81 Трудового кодекса РФ (разглашение охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей). А дальше…
На основании судебного решения уволенный сотрудник восстановлен на работе, компания оплатила ему не только вынужденный прогул, но и выплатила компенсацию за нанесенный сотруднику моральный вред. Начальник отдела и специалист службы технической поддержки осуждены по ч.2 ст.138 Уголовного кодекса РФ — оштрафованы на 100 тысяч рублей каждый.
Где справедливость?
Справедливость в том, что отсутствие правовых режимов защиты информации является сегодня типичной проблема российских компаний.
Применительно к рассмотренной ситуации мы, вроде бы, понимаем, что начальник имеет право смотреть переписку компании с клиентом, так как это надо ему для обеспечения деятельности фирмы. Мы также понимаем, что сотрудник, «сливающий» тайны фирмы конкурентам, должен быть наказан и уволен с соответствующей формулировкой. Однако для того, чтобы справедливость торжествовала не «по понятиям», а по Закону, владельцы конфиденциальной информации, особенно работодатели, обязаны предпринимать целый комплекс юридических мер, которые как раз и направлены на обеспечение конфиденциальности «закрытых» сведений.
Юридические меры защиты информации обладают рядом признаков, которые отличают их от прочих видов защиты данных: организационных, физических, технических. Юридические средства защиты не могут физически схватить за руку злоумышленника или преградить ему доступ к секретам фирмы. Юридические средства выполняют особые функции, позволяющие им занимать свое особое место в корпоративной системе защиты информации. С одной стороны, юридические меры выполняют охранительную функцию.

Они формируют отношение субъектов оборота информации к нормам и правилам такого оборота: «Не нарушай! За нарушение накажут по всей строгости Закона». С другой стороны — компенсационная функция: в случае нанесения вреда законному владельцу информации Закон привлекает нарушителя к ответственности и обязывает его возместить причиненный ущерб.

Использование подобного дуализма правовых режимов позволяет компаниям достаточно эффективно «достраивать» имеющиеся организационно-технические комплексы защиты информации до полноценных корпоративных Систем Безопасности Информации.

Надо также добавить, что именно правовые меры лучше всего воздействуют на наиболее «рисковые» группы субъектов информационного оборота — собственных сотрудников и контрагентов компании, доступ которых к конфиденциальным сведениям предусмотрен выполняемыми должностными обязанностями или договорными обязанностями.

Юридические средства защиты данных становятся в последнее время все более действенными, в частности, потому, что российский законодатель уделяет все больше внимания правовому регулированию вопросов информационной безопасности, в том числе, развитию института охраняемой законом тайны. Правовые режимы защиты информации на предприятии — это уже не желание руководства, а требование закона. Например, обязательным для предприятия является наличие правовых режимов защиты персональных данных работников, защиты профессиональной тайны, а также защиты конфиденциальных сведений, полученных в ходе осуществления совместной деятельности с другими организациями. Грамотно организованный режим защиты коммерческой тайны позволит возместить ущерб от ее незаконного разглашения. Положение о средствах коммуникации позволит предприятию осуществлять полноценное использование своей электронной почты, а положение о видеозаписи — устанавливать камеры наружного слежения. Дополнительно дисциплинирует персонал памятка об ответственности за неправомерное обращение с информацией. Несколько десятков локальных правовых актов, разработанных и принятых в организации, существенно снизят риски, связанные с неправомерным обращением с вашей информацией, и риски, возникающие у предприятия вследствие нарушения им норм российского законодательства, регулирующих обращение с охраняемыми сведениями.

Правда, надо признать, что «ситуация с тайнами» в российском праве еще очень далека от идеала (чего, например, стоит одно объединение в единой статье гражданского кодекса РФ коммерческой и служебной тайн).

Вопрос 2. Ловушки испытательного срока

Статья 70 "Испытание при приеме на работу" из Трудового кодекса РФ

...Испытание при приеме на работу не устанавливается для:

- лиц, поступающих на работу по конкурсу на замещение соответствующей должности, проведенному в порядке, установленном законом;
- беременных женщин;
- лиц, не достигших возраста восемнадцати лет;
- лиц, окончивших образовательные учреждения начального, среднего и высшего профессионального образования и впервые поступающих на работу по полученной специальности;
- лиц, избранных (выбранных) на выборную должность на оплачиваемую работу;
- лиц, приглашенных на работу в порядке перевода от другого работодателя по согласованию между работодателями;

в иных случаях, предусмотренных настоящим Кодексом, иными федеральными законами и коллективным договором.

Правила испытания

Прежде чем окончательно решить для себя дилемму, устанавливать или нет соискателю испытательный срок, необходимо взвесить все за и против. Если ваш выбор будет все же в

пользу установления испытательного срока, помните: уволить работника по его результатам весьма и весьма непросто.

Какие предписания дает нам на этот счет закон? Первое, что непременно следует знать кадровику, - такого рода проверка устанавливается лишь по соглашению сторон. Если кандидат возражает относительно данного условия, ни о каком испытательном сроке не может быть и речи. Далее, положение об испытательном сроке в обязательном порядке включается в текст трудового договора. Если упустите из виду этот момент, считайте, что работник принят в организацию без испытательного срока, даже если данное условие отражено в приказе о приеме на работу.

А теперь поговорим ***о допустимых сроках испытания.***

По общему правилу, предусмотренному законодателем (ст. 70 ТК РФ), этот период не должен превышать трех месяцев. Исключение сделано лишь для руководителей организаций, главных бухгалтеров и их заместителей, а также для руководителей филиалов, представительств и иных обособленных структурных подразделений. Испытание деловых и профессиональных качеств этих работников может длиться до шести месяцев.

Та же статья 70 ТК РФ устанавливает круг лиц, которым работодатель вообще не вправе предлагать испытательный срок при приеме на работу. Это беременные женщины, подростки, не достигшие 18 лет, сотрудники, приглашенные на работу в порядке перевода от другого работодателя, а также молодые специалисты, впервые поступающие на работу по специальности.

Ближе к концу испытательного срока нужно определиться с дальнейшей судьбой работника. Если его профессиональные качества окажутся неудовлетворительными, организация имеет право, предупредив работника в письменной форме за три дня до окончания испытательного срока, расторгнуть с ним трудовой договор. Причем необходимо четко изложить причины, послужившие основанием для признания работника не выдержавшим испытание.

Расторжение трудового договора по данному основанию осуществляется без учета мнения профсоюза и без выплаты выходного пособия (ч. 2 ст. 71 ТК РФ).

Если в период испытательного срока сам сотрудник пришел к выводу, что выполняемая работа не устраивает его по каким-либо причинам, он имеет право расторгнуть трудовой договор по собственному желанию, также в письменной форме предупредив работодателя за три дня.

Ошибки, ведущие в суд

Порой, игнорируя то или иное предписание закона или слишком вольно трактуя правовую норму, работодатель сам загоняет себя в ловушку. Это утверждение в полной мере относится и к процедуре установления испытательного срока.

Давайте проанализируем несколько типичных ошибок, способных создать конфликтную ситуацию в отношениях с работником и поставить организацию в положение ответчика на судебном процессе.

Ошибка первая. Работодатель с целью проверки предлагает соискателю заключить срочный трудовой договор.

Позиция организации ясна - если сотрудник не понравится, с ним можно расстаться без особых усилий. Ведь по истечении срока договора испытуемый перестанет иметь какое-либо отношение к организации.

Однако срочный трудовой договор может быть заключен лишь в случаях, прямо предусмотренных законом (ст. 58 и 59 ТК РФ)*. Судите сами: "Запрещается заключение срочных трудовых договоров в целях уклонения от предоставления прав и гарантий, предусмотренных работникам, с которыми заключается трудовой договор на неопределенный срок". Пленум Верховного суда РФ в своем постановлении от 17.03.04 № 2 рекомендовал судам обращать на это особое внимание. И если работник обратится в суд или Рострудинспекцию с жалобой на неправомерность ваших действий, договор может

быть признан заключенным на неопределенное время. Поэтому советуем вам не подменять испытательный срок срочным трудовым договором.

Ошибка вторая. При оформлении на работу в текст трудового договора не вносится положение об испытательном сроке.

Оно всплывает лишь позднее, при издании соответствующего приказа, что совершенно недопустимо. Любой правовой инспектор, сличив экземпляр трудового договора с текстом приказа, сочтет это грубым нарушением трудового законодательства. Суд (в случае возникновения трудового спора) посчитает условие об испытании недействительным. Ведь в законодательстве прямо сказано, что при установлении испытательного срока необходимо желание обеих сторон - как работодателя, так и работника. А документом, отражающим обоюдное волеизъявление, является именно трудовой договор, а не приказ.

Ошибка третья. На период испытательного срока работнику существенно занижается заработная плата, и это условие прямо оговаривается в трудовом договоре.

В период испытательного срока на работника распространяются все положения федеральных законов, иных нормативных правовых актов, локальных актов, а также коллективных соглашений и договоров при условии, что в них содержатся нормы трудового права. Между тем такая практика прямо противоречит статье 135 ТК РФ. Из текста этой статьи следует, что условия оплаты труда, определенные трудовым договором, не могут быть ухудшены по сравнению с действующим законодательством. В законе не сказано, что на период испытательного срока оплата труда работника имеет какую-либо специфику. Вернуть недоплаченные суммы в судебном порядке вашему работнику ничего не стоит, а для вас это ненужное разбирательство и лишняя головная боль.

Ошибка четвертая. Здесь речь пойдет не об одной ошибке, а сразу о нескольких. Они напрямую связаны с невнимательным прочтением правил и установок, четко прописанных в нормах трудового права. Так, нередки случаи, когда испытание устанавливается для лиц, по закону освобожденных от предварительной проверки своих профессиональных качеств. Или когда испытательный срок по времени превышает предельно допустимый. Многие кадровики старой школы по ошибке применяют 6-месячный срок испытания как общеустановленный (такой период был раньше предусмотрен в КЗоТе). Надо ли говорить, что такие явные проколы вряд ли ускользнут от внимания трудового инспектора!

Ошибка пятая. Несоблюдение срока и формы предупреждения работника о предстоящем увольнении.

Как мы уже отмечали выше, работодатель вправе определить и принять решение о несоответствии работника порученной ему трудовой функции только в период срока, установленного для испытания. Признав результаты испытания неудовлетворительными, он должен действовать строго в рамках части 1 статьи 71 ТК РФ, то есть за три дня до окончания испытания предупредить сотрудника о своем намерении расторгнуть с ним трудовой договор. Причем такое предупреждение нужно оформить в письменном виде. Несоблюдение установленного порядка может иметь для работодателя негативные последствия: "Если срок испытания истек, а работник продолжает работу, то он считается выдержавшим испытание и последующее расторжение трудового договора с ним допускается только на общих основаниях" (ст. 71 ТК РФ). Другими словами, если вы не хотите, чтобы после испытательного срока сотрудник оставался в вашей организации, соблюдайте процедуру предупреждения об увольнении.

Ошибка шестая. При формулировке причин неудовлетворительных результатов испытания (они излагаются в письменном виде и вручаются работнику) допускается неаргументированная, некорректная, юридически несостоятельная форма изложения.

Такую ошибку работодатели допускают вследствие того, что у них отсутствует доказательственная база для подтверждения неудовлетворительного результата испытания

и они просто не знают, чем объяснять свое решение. Помните, что к сомнительным формулировкам суд относится критически. Поэтому здесь нужно быть предельно внимательными и учитывать, что любое действие руководителя в отношении подчиненного, тем более действие, способное породить конфликтную ситуацию, должно быть определенным образом оформлено и "запротоколировано". Только таким образом в случае судебного разбирательства можно отбить атаки обиженного работника. Об этом поговорим подробнее.

Ошибка седьмая. Работодатель не может подтвердить правомерность своих действий.

Именно представителю организации в ходе судебного заседания придется доказывать обоснованность увольнения работника. При увольнении подчиненного по статье 71 ТК РФ работодателю следует четко помнить - основанием для расторжения трудового договора в данном случае может быть лишь ссылка на ненадлежащие деловые качества работника. То есть на низкий уровень профессионализма или на неудовлетворительные для данной работы личностные характеристики сотрудника (например, недостаточно быстрая реакция при работе в экстремальных ситуациях), или на отсутствие должной трудовой дисциплины. Причем, как мы уже говорили, все утверждения работодателя должны быть подтверждены соответствующими реальными доказательствами.

К числу таких доказательств можно отнести документальное оформление дисциплинарного проступка (объяснительная, акты, приказ о наложении взыскания), а также доказательства, подтверждающие ненадлежащее исполнение трудовой функции, в том числе невыполнение норм выработки и несоблюдение нормативов времени (письменное задание руководителя и отчет сотрудника о его выполнении, жалобы клиентов и коллег и т. п.).

Вопрос 3. Обязанности сотрудников предприятия работающих со сведениями, представляющими коммерческую тайну, и их ответственность за ее разглашение.

Сотрудники предприятия, допущенные к сведениям, составляющим коммерческую тайну, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений.

До получения доступа к работе, связанной с коммерческой тайной, им необходимо изучить настоящую инструкцию и дать в службе безопасности письменное обязательство о сохранении коммерческой тайны.

Сотрудники предприятия, допущенные к коммерческой тайне должны:

Строго хранить коммерческую тайну. О ставших им известной утечке сведений, составляющих коммерческую тайну, а также об утрате документов с грифом "КТ", сообщать непосредственному руководителю и в службу безопасности.

Предъявлять для проверки по требованию представителей службы безопасности все числящиеся документы с грифом "КТ", а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения.

Знакомиться только с теми документами и выполнять только те работы, к которым они допущены.

Строго соблюдать правила пользования документами, имеющими гриф "КТ". Не допускать их необоснованной рассылки.

Все полученные в делопроизводстве службы безопасности или у ее уполномоченного документы с указанным грифом немедленно вносить во внутреннюю опись документов (форма 55), а которой отводится специальный раздел по учету "КТ".

Исполненные входящие документы, а также документы, предназначенные для рассылки, подшивки в дело или уничтожения сдавать в делопроизводство службы безопасности или уполномоченному службы безопасности.

Выполнять требования внутри объектного режима: исключающие возможность ознакомления с документами "КТ" посторонних лиц, включая и своих сотрудников, не имеющих к указанным документам прямого отношения.

При ведении деловых переговоров с представителями сторонних организаций или

частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения.
Исключить использование ставшей известной коммерческой тайны предприятия в свою личную пользу, а также деятельность, которая может быть использована конкурентами в ущерб предприятию владельцу данной коммерческой тайны.
Ответственность за разглашение сведений, составляющих коммерческую тайну предприятия, и утрату документов или изделий, содержащих такие сведения устанавливается в соответствии с действующим законодательством.
При этом подразумевается:
Под разглашением сведений, составляющих коммерческую тайну - предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц.
Под утратой документов или изделий (предметов), содержащих сведения, относящиеся к коммерческой тайне, - выход (в том числе и временный) документов или изделий из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или изделия стали либо могли стать достоянием посторонних лиц.

Литература

1. Афанасьев В.Г. Системность и общество. - М.: Политиздат, 2013, с. 24.
2. Альбрехт У., Венц Дж., Уильямс Т. Мошенничество. - СПб: Питер Пресс, 2016, с. 398-404.
3. Ларичев В. Д. Как уберечься от мошенничества в сфере бизнеса. - М.: Юристъ, 2014, с. 118-120.
4. Ольшаный А.И. Банковское кредитование: российский и зарубежный опыт. - М.: Русская Деловая Литература, 2014, с. 288.
5. Ярочкин В.И. Секьюритология - наука о безопасности жизнедеятельности. - М.: "Ось-89", 2021, с. 151.
6. Гражданский кодекс РФ
7. Трудовой Кодекс РФ

Лабораторное занятие №6.
Тема: Разработка инструкции по обеспечению сохранности конфиденциальной информации на предприятии

Содержание занятия

Инструкция по обеспечению сохранности конфиденциальной информации на предприятии

1. Общие положения.
2. Определение информации и обозначение документов, содержащих коммерческую тайну, и сроков ее действия
3. Организация работы с документами, имеющими гриф "КОММЕРЧЕСКАЯ ТАЙНА".
4. Порядок сохранности документов, дел и изданий.
5. Порядок допуска к сведениям, составляющим коммерческую тайну предприятия.
6. Контроль за выполнением требований внутри объектного режима при работе со сведениями содержащими коммерческую тайну.
7. Обязанности сотрудников предприятия, работающих со сведениями представляющими коммерческую тайну, и их ответственность за ее разглашение.
8. Перечень сведений, составляющих коммерческую тайну предприятия.
9. Положение о службе безопасности предприятия.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция разработана в соответствии с требованиями законов РСФСР "О предприятиях и предпринимательской деятельности", закона РФ о КТ и Устава предприятия. Предусматривает административные и экономические о защиты коммерческой тайны предприятия с целью предотвращения нанесения возможного экономического и морального ущерба предприятию со стороны юридических и физических лиц, вызванного их неправомерными или не осторожными действиями путем безвозмездного присвоения чужой информации или разглашения коммерческой тайны.

Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам. К сведениям, составляющим коммерческую тайну, относятся несекретные сведения, предусмотренные " Перечнем сведений, составляющих коммерческую тайну предприятия", утвержденным и введенным в действие приказом руководителя предприятия Коммерческая тайна предприятия является его собственностью. Если она представляет собой результат совместной деятельности с другими предприятиями, основанной на договорных началах, то коммерческая тайна может быть собственностью двух сторон, что должно найти отражение в договоре.

Под разглашением коммерческой тайны подразумевается умышленные или неосторожные действия должностных или иных физических лиц, приведшие к не вызванному служебной необходимостью или преждевременному открытому опубликованию сведений, подпадающих под категорию сведений, составляющих коммерческую тайну, а также передача подобных сведений по открытым техническим каналам связи или их обработка на некатегорированных СВТ.

Под открытым опубликованием таких сведений подразумевается их публикация в открытой печати, передача по радио и телевидению, оглашение на международных, зарубежных и открытых внутрироссийских симпозиумах, совещаниях, конференциях, съездах, при публичных вступлениях и защите диссертаций, вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным

лицам.
Необходимость открытого опубликования сведений, составляющих коммерческую тайну, их объемы, формы и время опубликования определяются руководителем предприятия с учетом заключения постоянно действующей экспертной комиссии.
Использование для открытого опубликования сведений, полученных на договорной или доверительной основе или являющихся результатом совместной деятельности, допускается только с общего согласия партнеров.
Меры по ограничению открытых публикаций коммерческой информации не могут быть использованы для сокрытия от общественности фактов злоупотреблений, расточительства, бесхозяйственности, недобросовестной конкуренции и других негативных явлений в деятельности предприятия. При определении сведений, которые не могут составлять коммерческую тайну необходимо руководствоваться законом РФ о КТ (2004 г.)
Передача информации сторонним организациям, с которыми предприятие не связано прямыми служебными контактами, должна регулироваться, как правило, договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат за предоставление информации и компенсацию за нарушение договорных обязательств.
Предоставление коммерческой информации представителям служебных, ревизионных, фискальных и следственных органов, народным депутатам, органам печати, радио, телевидения и т.п. регулируется соответствующими положениями.
Тиражированные документы и издания с грифом "КОММЕРЧЕСКАЯ ТАЙНА" ("КТ") рассматриваются как материалы, содержащие сведения ограниченного распространения.
Защита коммерческой тайны предусматривает:
порядок определения информации, содержащей коммерческую тайну, и сроков ее действия
систему допуска сотрудников предприятия, частных и командированных лиц к сведениям, составляющим коммерческую тайну предприятия
обязанности лиц, допущенных к таким сведениям порядок работы с документами, имеющими гриф "КТ"
обеспечение сохранности документов, дел и изданий с грифом "КТ"
принципы организации и проведения контроля за обеспечением установленного порядка при работе со сведениями, составляющими коммерческую тайну
ответственность за разглашение сведений и утрату документов, содержащих коммерческую тайну.
Ответственность за организацию работы с материалами, имеющими гриф "КТ", разработку и осуществление необходимых мер по сохранности коммерческой тайны руководитель предприятия возлагает на ответственных руководителей направлений и структурных подразделений
Контроль за осуществлением мер, обеспечивающих сохранность коммерческой тайны, возлагается на службу безопасности предприятия которая силами:
Первого отдела - контролирует, а в необходимых случаях обеспечивает учет, размножения и хранения документов, дел и изданий с грифом коммерческая тайна".
Подразделений режима - контролирует, а в необходимых случаях через уполномоченных служб безопасности обеспечивает сохранность коммерческой тайны путем максимального ограничения круга лиц, допущенных к коммерческой тайне предприятия, выполнение требований при обработке информации с грифом "КТ" на защищенных СВТ, а также требований по конфиденциальности конкретной информации, внесенных в договора со сторонними предприятиями - партнерами.

2. ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ И ОБОЗНАЧЕНИЕ ДОКУМЕНТОВ, СОДЕРЖАЩИХ КОММЕРЧЕСКУЮ ТАЙНУ, И СРОКОВ ЕЕ ДЕЙСТВИЯ.

Необходимость проставления грифа "Коммерческая тайна" ("КТ") определяется в

соответствии с Перечнем, указанным в п.1.2 настоящей Инструкции: при работе с документом-исполнителем и лицом, подписывающим документ, при работе с изданием-автором (составителем) и руководителем, утверждающим издание к печати.
На документах, делах и изданиях, содержащих сведения, составляющие коммерческую тайну, проставляется гриф "Коммерческая тайна" ("КТ"), а на документах и изданиях, кроме того, - номера экземпляров. Гриф и номера экземпляров, проставляются в правом верхнем углу первой страницы документа, на обложке или титульном листе издания и на первой странице сопроводительного письма к этим материалам. На обратной стороне последнего листа каждого экземпляра печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фамилия исполнителя и его телефон, дата, фамилия машинистки и срок действия коммерческой тайны (регистрационный номер проставляется на каждом листе документа).
Срок действия коммерческой тайны, содержащейся в документе, определяется в каждом конкретном случае исполнителем или лицом, подписавшем документ, в виде конкретной даты или в виде пометок: "до заключения контракта", "бессрочно" и т.п.
Основанием для снятия грифа "Коммерческая тайна" является решение постоянно действующей экспертной комиссии, оформляемым актом, утвержденным руководителем предприятия. К работе комиссии привлекаются представители заинтересованных структурных подразделений. Один экземпляр акта вместе с делами передается в архив предприятия, а на деле постоянного хранения в государственных архив.
Гриф "КТ" после оформления его снятия (п. 2.4) погашается штампом или записью о руки с указанием даты и номера акта, послужившего основанием для его снятия. Аналогичные отметки вносятся в описи и номенклатуры дел.

3. ОРГАНИЗАЦИЯ РАБОТЫ С ДОКУМЕНТАМИ, ИМЕЮЩИМИ ГРИФ "КОММЕРЧЕСКАЯ ТАЙНА" ("КТ")

Документы, имеющие гриф "КТ", подлежат обязательной регистрации в подразделении делопроизводства службы безопасности (в Первом отделе) или в общем делопроизводстве производственного подразделения уполномоченным службы безопасности. Эти документы должны иметь реквизиты, предусмотренные п.2.2 и гриф "КТ" (или полностью "Коммерческая тайна").
Права на информацию, порядок пользования ею, сроки ограничения на публикацию могут оговариваться дополнительно в тексте документа и его реквизитах.
Отсутствие грифа "КТ" и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и лицо, подписавшее или утвердившее документ, предусмотрели возможные последствия от свободной рассылки и несут за это ответственность.
Вся поступающая корреспонденция, имеющая гриф "КТ" (или другие соответствующие этому понятию грифы, например, "секрет предприятия, "тайна предприятия" и др.) принимается и вскрывается сотрудниками предприятия, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров, а также наличие указанных в сопроводительном письме приложений. При обнаружении отсутствия в конвертах (пакетах) указанных документов составляется акт в 2-х экземплярах: один экземпляр акта направляется отправителю.
Все входящие, исходящие и внутренние документы, а также издания с грифом "КТ" подлежат регистрации и учитываются по количеству листов, а издания - поэкземплярно.
Учет документов и изданий с грифом "КТ" ведется в журналах или карточках отдельно от учета другой служебной несекретной документации. Листы журналов нумеруются, прошиваются и опечатываются. Документы, которые не подшиваются в дела, учитываются в журнале инвентарного учета.
Движение документов и изданий с грифом "КТ" своевременно отражается в журналах или карточках.
На зарегистрированном документе с грифом "КТ" (или на сопроводительном листе к

изданиям с грифом "КТ") должен быть проставлен штамп с указанием наименования предприятия, регистрационный номер документа и дата его поступления.
Издания с грифом "КТ" регистрируются в журнале учета и распределения изданий.
Отпечатанные и подписанные документы вместе с их черновиками передаются для регистрации сотруднику подразделения делопроизводства службы безопасности, осуществляющему их учет. Черновики уничтожаются исполнителем и этим сотрудником, что подтверждается росписью указанных лиц в журнале или на карточках учета. При этом проставляется дата и подпись.
Размножение документов и изданий с грифом "КТ" в типографиях и других множительных участках производится с разрешения и под контролем специально назначенных сотрудников службы безопасности по заказам, подписанным руководителем предприятия.
Размноженные документы "КТ" (копии, тираж) должны быть полистно подобраны, пронумерованы поэкземплярно и, при необходимости, сброшюрованы (сшиты). Нумерация дополнительно размноженных экземпляров, производится от последнего номера, ранее учтенных экземпляров этого документа.
Перед размножением на последнем листе оригинала (подлинника) проставляется запись: " Регистрационный номер_____.
Дополнительно размножено_____экз., на _____листах текста. Наряд N ____от _____. Подпись (" исполнитель заказа) ". Одновременно делается отметка об этом в соответствующих журналах и карточках учета.
Рассылка документов и изданий с грифом "КТ" производиться на основании подписанных руководителем структурного подразделения разнарядок с указанием учетных номеров отправляемых экземпляров.
Пересылка пакетов с грифом "КТ" может осуществляться через органы спецсвязи или фельдсвязи.
Документы с грифом "КТ" после исполнения группируются в отдельные дела. Порядок их группировки предусматривается специальной номенклатурой дел, в которую в обязательном порядке включаются все справочные картотеки и журналы на документы и издания с грифом "КТ".
Снятия рукописных, машинописных, микро - и фотокопий, электрографических и др. копий, а также производство выписок из документов и изданий с грифом "КТ" сотрудниками предприятия производится по разрешению руководителя предприятия и подразделений.
Обработка информации с грифом "КТ" производится на учетных СВТ, которые имеют категорию не ниже 4-Б.

4. ПОРЯДОК ОБЕСПЕЧЕНИЯ СОХРАННОСТИ ДОКУМЕНТОВ, ДЕЛ И ИЗДАНИЙ

Все имеющие гриф "КТ" документы, дела и издания должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. Помещения должны отвечать требованиям внутри объектного режима, обеспечивающего физическую сохранность находящейся в них документации.
Дела с грифом "КТ", выдаваемые исполнителю, подлежат возврату в подразделение делопроизводства службы безопасности (СБ) в тот же день. При необходимости, с разрешения начальника подразделения делопроизводства СБ или уполномоченного СБ они могут находиться у исполнителя в течении срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.
С документацией с грифом "КТ" разрешается работать только в служебных помещениях. Для работы вне служебных помещений необходимо разрешение руководителя предприятия или структурного подразделения.
Документы, дела и издания с грифом "КТ" могут передаваться другим сотрудникам,

допущенным к этим документам, только через делопроизводство СБ или уполномоченного СБ.
Изъятия из дел или перемещение документов с грифом "КТ" из одного дела в другое без санкции руководителя делопроизводства СБ или уполномоченного СБ, осуществляющего их учет, запрещается.
Смена сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом "КТ", оформляется распоряжением начальника подразделения. При этом составляется по произвольной форме акт приема- передачи этих материалов, утверждаемый указанным руководителем.
Уничтожение документов "КТ" производится комиссией в составе не менее трех человек с составлением акта.
Печатание документов "КТ" разрешается в машинописном бюро или непосредственно в подразделениях. Для учета отпечатанных документов ведется специальный журнал.

5. ПОРЯДОК ДОПУСКА К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ КОММЕРЧЕСКУЮ ТАЙНУ ПРЕДПРИЯТИЯ

Допуск сотрудников к сведениям, составляющим коммерческую тайну, осуществляется руководителем предприятия или руководителями его структурных подразделений.
Руководители подразделений и службы безопасности обязаны обеспечить систематический контроль за допуском к этим сведениям только тех лиц, которым они необходимы для выполнения служебных обязанностей.
К сведениям, составляющим коммерческую тайну, допускаются лица, личные и деловые качества которых обеспечивают их способность хранить коммерческую тайну, и только после оформления в службе безопасности письменного обязательства по сохранению коммерческой тайны.
Допуск сотрудников к работе с делами "КТ" осуществляется согласно оформленному не внутренней стороне обложки дела или на отдельном листе списку за подписью руководителя предприятия структурного подразделения, а к документам - в соответствии с указаниями, содержащимися в резолюциях руководителей предприятия и подразделений.
Представители сторонних организаций и частные лица могут быть допущены к ознакомлению и работе с документами и изданиями с грифом "КТ" с письменного разрешения руководителей предприятия или подразделений, в ведении которых находятся эти материалы.
Выписки из документов и изданий, содержащих сведения с грифом "КТ", производятся в блокнотах (или тетрадях), которые имеют такой же гриф. После окончания работы они высылаются в адрес той организации, которая будет указана данным представителем.
Выдача дел и изданий с грифом "КТ" исполнителям и прием от них производится под расписку в "Карточке учета выдаваемых дел и изданий."
Дела и издания непосредственно представителям сторонних организаций и частным лицам не выдаются. При необходимости с их содержанием они ознакомятся только с разрешения руководителя предприятия через уполномоченного службы безопасности или представителя заинтересованного подразделения.

6. КОНТРОЛЬ ЗА ВЫПОЛНЕНИЕМ ТРЕБОВАНИЙ ВНУТРИОБЪЕКТОВОГО РЕЖИМА ПРИ РАБОТЕ СО СВЕДЕНИЯМИ СОДЕРЖАЩИМИ КОММЕРЧЕСКУЮ ТАЙНУ.

Под внутри объектовым режимом при работе с коммерческой тайной подразумевается соблюдение условий работы, исключающих возможность утечки информации о сведениях, содержащих коммерческую тайну.
Контроль за соблюдением указанного режима осуществляется в целях изучения и оценки состояния сохранности коммерческой тайны, выявления и установления причин недостатков, и выработки предложений по их устранению.
Контроль за обеспечением режима при работе со сведениями, содержащими

коммерческую тайну, осуществляют служба безопасности предприятия и руководитель структурного подразделения путем текущих и плановых проверок.
При проведении проверок создается комиссия, которая комплектуется из опытных и квалифицированных работников в составе не менее двух человек, допущенных к работе с материалами "КТ".
Участие в проверке не должно приводить к необоснованному увеличению осведомленности в этих сведениях.
Плановые проверки проводятся не реже одного раза в год комиссиями на основании приказа или распоряжения руководителя предприятия (подразделения).
Проверяющие имеют право знакомиться со всеми документами, журналами (карточками) и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы, консультироваться со специалистами и исполнителями, требовать представления письменных объяснений, справок и отчетов по всем вопросам, входящим в компетенцию комиссии.
При проверках присутствует руководитель структурного подразделения или его заместитель.
По результатам проверок составляется акт или справка с отражением в нем наличия документов, состояния работы с материалами "КТ", выявленных недостатков и предложений по их устранению. Акт утверждается руководителем предприятия (подразделения).
При выявлении случаев утраты документов или разглашения сведений, составляющих коммерческую тайну, ставятся в известность руководитель предприятия и его заместитель (помощник) по безопасности. Для расследования указанных случаев приказом руководителя предприятия создается комиссия, которая:
определяет соответствие содержания утраченного документа проставленному грифу "КТ" и выявляет обстоятельства утраты (разглашения). По результатам работы комиссии составляется акт.

7. ОБЯЗАННОСТИ СОТРУДНИКОВ ПРЕДПРИЯТИЯ РАБОТАЮЩИХ СО СВЕДЕНИЯМИ, ПРЕДСТАВЛЯЮЩИМИ КОММЕРЧЕСКУЮ ТАЙНУ, И ИХ ОТВЕТСТВЕННОСТЬ ЗА ЕЕ РАЗГЛАШЕНИЕ.

Сотрудники предприятия, допущенные к сведениям, составляющим коммерческую тайну, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений.
До получения доступа к работе, связанной с коммерческой тайной, им необходимо изучить настоящую инструкцию и дать в службе безопасности письменное обязательство о сохранении коммерческой тайны.
Сотрудники предприятия, допущенные к коммерческой тайне должны:
Строго хранить коммерческую тайну. О ставших им известной утечке сведений, составляющих коммерческую тайну, а также об утрате документов с грифом "КТ", сообщать непосредственному руководителю и в службу безопасности.
Предъявлять для проверки по требованию представителей службы безопасности все числящиеся документы с грифом "КТ", а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения.
Знакомиться только с теми документами и выполнять только те работы, к которым они допущены.
Строго соблюдать правила пользования документами, имеющими гриф "КТ". Не допускать их необоснованной рассылки.
Все полученные в делопроизводстве службы безопасности или у ее уполномоченного документы с указанным грифом немедленно вносить во внутреннюю опись документов (форма 55), а которой отводится специальный раздел по учету "КТ".
Исполненные входящие документы, а также документы, предназначенные для рассылки, подшивки в дело или уничтожения сдавать в делопроизводство службы безопасности или

уполномоченному службы безопасности.
Выполнять требования внутри объектного режима: исключающие возможность ознакомления с документами "КТ" посторонних лиц, включая и своих сотрудников, не имеющих к указанным документам прямого отношения.
При ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения.
Исключить использование ставшей известной коммерческой тайны предприятия в свою личную пользу, а также деятельность, которая может быть использована конкурентами в ущерб предприятию - владельцу данной коммерческой тайны.
Ответственность за разглашение сведений, составляющих коммерческую тайну предприятия, и утрату документов или изделий, содержащих такие сведения устанавливается в соответствии с действующим законодательством.
При этом подразумевается:
Под разглашением сведений, составляющих коммерческую тайну - предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц.
Под утратой документов или изделий (предметов), содержащих сведения, относящиеся к коммерческой тайне, - выход (в том числе и временный) документов или изделий из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или изделия стали либо могли стать достоянием посторонних лиц.

ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ ПРЕДПРИЯТИЯ.

Общие положения

Перечень сведений, составляющих коммерческую тайну предприятия, составлен в соответствии с требованиями закона РСФСР " О предприятиях и предпринимательской деятельности" Закона РФ о КТ и Устава предприятия.
В настоящем перечне предусматриваются категории не секретных сведений, связанных с научно-исследовательской и производственно- технической деятельностью предприятия, разглашение которых может нанести материальный, моральный или иной ущерб интересам предприятия.
При простановке грифа " Коммерческая тайна" ("КТ") основное внимание должно быть уделено обеспечению сохранности действительно важной для предприятия коммерческой информации и вместе с тем созданию условий для более широкого использования новейших достижений науки и техники.
В этих же целях Перечнем устанавливается ориентировочный срок действия грифа "КТ".
Сведения, указанные в настоящем Перечне, не подлежат передаче или разглашению другим предприятиям и частным лицам без разрешения руководителя предприятия.
Гриф "КТ" проставляется конкретным исполнителем и руководителем подразделения, которые несут ответственность за правильность определения объема сведений, составляющих коммерческую тайну. При этом они должны руководствоваться настоящим Перечнем, а также Перечнем сведений, которые не могут составлять коммерческую тайну.
Гриф "КТ" печатается в правом верхнем углу титульного листа каждого экземпляра. Ниже печатается экз. N. На оборотной стороне последнего листа каждого экземпляра печатаются данные: количество отпечатанных экземпляров,
Регистрационный номер, фамилия исполнителя, его телефон, дата, фамилия машинистки.

Перечень категорий сведений, составляющих коммерческую тайну предприятия

1. ОБЩИЕ ПОЛОЖЕНИЯ

В настоящем перечне указываются категории несекретных сведений, связанных с экономической, производственной, научно-технической, валютно- финансовой и

внешнеэкономической деятельностью предприятия, разглашение которых может нанести материальный, моральный или иной ущерб интересам предприятия.
Сведения, предусмотренные в настоящем Перечне, не подлежат передаче или разглашению другим предприятиям, организациям и частным лицам без разрешения руководителя предприятия.
Конкретные исполнители и руководители подразделений несут ответственность за правильность определения объема сведений, составляющих коммерческую тайну. При этом они должны руководствоваться Настоящим Перечнем, а также Перечнем сведений, которые не могут составлять коммерческую тайну, введенным в действие Постановлением правительства РСФСР от 5 декабря 1991 года N 35.
Срок действия коммерческой тайны предприятия определяется в каждом конкретном случае.
Понятия "Коммерческая тайна" основывается на конфиденциальности сведений, Отношений, переписки, переговоров между сторонами сделки и затрагивает только интересы предприятия.

2. ПЕРЕЧЕНЬ КАТЕГОРИЙ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ ПРЕДПРИЯТИЯ

Научно-техническая деятельность
Материалы об открытиях и изобретениях, сделанных на предприятии и имеющих крупное научное значение.
Конкретные сведения о контрагентах и исполнителях НИР и ОКР, выполняемых ими работах, их полные названия и принадлежность.
Сведения о схемно-конструктивных решениях разрабатываемого изделия, придающих ему новые потребительские свойства, изменяющие стоимостные показатели.
Сведения по научно-техническим вопросам, касающиеся деятельности иностранных фирм, которыми конфиденциально располагает предприятия.
Информация о потенциальных заказчиках НИР и ОКР. Экономика и производство
Полные плановые или отчетные данные о вводе в действие основных фондов, об объемах капитальных вложений или строительно-монтажных работ.
Направления и объемы инвестиций.
Плановые экономические показатели, в том числе планируемая прибыль. Объемы сбыта и варианты реализации продукции на экспорт.
Уровень качества, организация работ по качеству, состояние работ по сертификации продукции, внедрение международных стандартов серии ИСО 9000.
Сведения о новых материалах, применяемых на предприятии, и технология их применения.
Обобщенные сведения о выгодных перспективных поставщиках материалов и комплектующих изделий и состоянии деловых отношений с ними.
Сведения о специальных комплектующих изделиях, придающих изготавливаемой продукции новые потребительские качества.
Сведения о предприятии как о торговом партнере.
Сведения о модернизации ранее известных технологий, процессов и оборудования, позволяющих повысить конкурентоспособность на внутреннем и внешнем рынке.
Фактические сведения о численности и фонде заработной платы работников предприятия.
Сведения о состоянии программного и компьютерного обеспечения (в т.ч. названия программ, фирмы-поставщики МПО, описание и назначение МПО, тексты программ, Реализующие новые и оригинальные научно- технические решения).
Валютно-финансовые вопросы.
Плановые или фактические объемы финансирования капитальных вложений, научно-исследовательских и опытно-конструкторских работ и затрат на внедрение новой техники по предприятию.
Плановые и фактические показатели финансового плана предприятия. Данные о балансе

доходов и расходов по предприятию.
Показатели рентабельности производства, прибыли, убытков по предприятию.
Сведения о размерах и условиях кредитов, полученных как у российских, так и у иностранных банков, организаций и фирм.
Сведения, раскрывающие директивы по проведению переговоров, в т.ч. границы полномочий должностных лиц по ценам, скидкам и другим условиям.
Сведения, раскрывающие генеральную линию и тактику в валютных и кредитных вопросах.
Порядок и объемы финансирования экспортных и импортных операций.
Результаты финансово-хозяйственной деятельности предприятия за квартал или год.
Технико-экономические расчеты по объектам, строящимся при техническом содействии иностранных фирм.
Данные, раскрывающие уровни и лимиты цен на товар, продажа которого на текущий год еще не закончена.
Расчеты экспортной и импортной стоимости оборудования и услуг.
Сведения о коэффициенте эффективности по поставкам оборудования и об эффективности сделки.
Сведения об эффективности экспорта и импорта.
Плановые и фактические показатели финансово-хозяйственной деятельности собственных и смешанных обществ с участием капитала предприятия, а также сведений о капиталах и доходах по этим обществам.
Сводные сведения о заработной плате сотрудников предприятия.
Сведения об участии предприятия как учредителя в акционерных обществах, совместных предприятиях, малых предприятиях и о размере капитала в уставном фонде.
Механизм образования цены на изделие (формирование цены; накладные расходы в составе договорной цены; составляющие накладных расходов).
Предполагаемые договорные цены на разработку или поставку изделий (или научно технической продукции).
Продажная стоимость конкретного изделия. Внешнеэкономическая деятельность
Позиция представителей предприятия при проведении торговых переговоров, разглашение которой может нанести ущерб предприятию.
Сведения о сроках, установленных для проработки и заключения сделки.
Сведения о получаемых и прорабатываемых заказах и предложениях иностранных фирм.
Сведения об объемах взаимных поставок по долгосрочным соглашениям с одной или несколькими фирмами.
Сведения, характеризующие иностранцев, иностранные фирмы или организации, технологию производства или конструкторские решения, применяемые ими, составленные на основании конфиденциально полученных данных.
Сведения, раскрывающие факт конфиденциальной договоренности сторон или ее содержание.
Сведения, на конфиденциальности которых настаивает иностранный партнер.
Сведения, раскрывающие существо позиции предприятия при ведении судебных и арбитражных дел за границей, разглашение которых может принести ущерб предприятию.
Сведения о предполагаемых закупках за границей отдельных патентов, лицензий и образцов техники.
Сведения о предполагаемых закупках (продажах), раскрывающие степень заинтересованности предприятия в импорте или экспорте отдельных видов товаров.
Содержание торговых соглашений, договоров или контрактов, которые по договоренности сторон следует считать конфиденциальными.
Сведения о характере технических заданий представителям предприятия, командируемым за границу, опубликование которых может нанести ущерб предприятию.

9. ПОЛОЖЕНИЕ О СЛУЖБЕ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ.

Служба безопасности (СБ) предприятия образована приказом директора N_____от _____ в целях защиты экономических интересов предприятия и обеспечения максимальной безопасности его деятельности как субъекта рыночных отношений.

СБ является самостоятельным подразделением и подчиняется непосредственно руководителю предприятия.

Руководство Службой осуществляет начальник СБ, который назначается и освобождается от занимаемой должности руководителем предприятия.

Структура и штаты СБ по представлению начальника утверждаются руководителем предприятия.

Деятельность СБ финансируется за счет включения ее затрат в себестоимость работ, выполняемых предприятием.

СБ в своей деятельности руководствуется законами Российской Федерации, указами Президента, постановлениями Совета Министров, ведомственными приказами и указаниями, Уставом предприятия, приказами и указаниями руководителя предприятия и настоящим Положением.

2. ОСНОВНЫЕ ЗАДАЧИ

Основными задачами СБ предприятия являются:

Обеспечение экономической безопасности, защиты собственности предприятия.

Организация делопроизводства.

Обеспечение мер защиты при использовании средств связи (телетайп, телекс, телефакс, телефон).

Организация противодействия техническим средствам разведки на объектах предприятия.

Обеспечение внутри объектового и пропускного режима, охрана имущества и персонала предприятия.

Обеспечение защиты охраняемой информации и экономической безопасности при осуществлении внешнеэкономической деятельности.

Оказание помощи структурным подразделениям в изучении конъюнктуры рынка, предполагаемых партнеров, конкурентов.

Контроль за выполнением нормативных документов, Выявление и закрытие возможных каналов утечки охраняемой информации в процессе производственной и иной деятельности предприятия.

Контроль за состоянием противопожарной безопасности на объектах предприятия.

3. ФУНКЦИИ

В соответствии с основными задачами СБ предприятия выполняет следующие функции:

По вопросам допуска сотрудников к охраняемой информации:

Совместно со специалистами, ответственными исполнителями разрабатывает перечень сведений, составляющих коммерческую тайну (КТ) предприятия. Вносит соответствующие документы на рассмотрение и утверждение руководителя. Контролирует соответствие содержания и условий проведения работ реквизиту "КТ - собственность предприятия" и сроки его действия.

Разрабатывает и осуществляет мероприятия., обеспечивающие доступ к охраняемой информации только тех лиц, которым это необходимо для выполнения служебных обязанностей.

Разрабатывает систему организационных и технических мер, регламентирующих внутри объектовый режим предприятия. Организует и контролирует их выполнение.

Осуществляет контроль за изготовлением, учетом, хранением, выдачей и использованием бланков служебных удостоверений (пропусков), печатей, штампов предприятия, а также металлических и мастичных печатей с индивидуальными учетными номерами.

По вопросам делопроизводства:

Организует и ведет делопроизводство; контролирует обеспечение установленного порядка

размножения документов, их учета, хранения и пользования ими.
Обеспечивает соблюдение правил рассылки документов, содержащих коммерческую тайну предприятия.
Разрабатывает и осуществляет меры по предотвращению разглашения и утечки информации при ведении делопроизводства.
3.3. По вопросам передачи и приема информации техническими средствами связи:
Организует прием и передачу охраняемой информации и открытой корреспонденции по телетайпу, телексу, телефаксу.
Выбирает эффективные и экономичные средства связи в зависимости от характера передаваемой информации. Учитывает и анализирует входящую и исходящую корреспонденцию, оперативно доводит до адресатов.
По вопросам обеспечения пропускного режима, охраны имущества и персонала предприятия, контроля за противопожарной безопасностью:
Разрабатывает документы, регламентирующие пропускной режим и утверждает их у руководителя предприятия. Оформляет, учитывает, выдает, изымает все виды пропусков на территорию предприятия. Контролирует правильность оформления документов на ввоз (вывоз), внос(вынос) материальных ценностей и документов.
Организует контрольно-пропускные посты. Обеспечивает установленный временной режим охраны объектов предприятия. Эксплуатирует технические средства охраны.
Разрабатывает и осуществляет меры по обеспечению личной безопасности работников предприятия.
Следит за состоянием противопожарной безопасности, предлагает меры по устранению нарушений.
По вопросам инженерно-технического обеспечения безопасности охраняемой информации и охраны предприятия:
Разрабатывает требования к помещениям, где ведутся работы с охраняемой информацией, хранятся соответствующие документы, изделия, а также материальные ценности. Проводит аттестацию помещений и объектов хранения материальных ценностей. Организует установку и эксплуатацию технических средств защиты, в том числе и средств противодействия техническим разведчикам (ПДТР)
Координирует меры безопасности при проведении работ с использованием ЭВТ. Организует спецпроверки и специсследования. Контролирует выполнение нормативных документов при эксплуатации ПЭВМ.
Ведет учет сейфов, металлических шкафов, специальных хранилищ (а также ключей к ним), в которых разрешено постоянно или временно хранить документы, содержащие охраняемую информацию (с реквизитом "КТ- собственность предприятия").
Контролирует выполнение заявок (договоров) на установку и ремонт инженерно-технических средств защиты, а также установку средств связи.
По вопросам безопасности информации при осуществлении внешнеэкономической деятельности:
Участвует в подборе специалистов, способных вести эффективную работу с зарубежными фирмами и в подготовке оформления выездных документов для загранкомандировок.
Участвует в подготовке документов и материалов (программы, соглашения, контракты) по внешнеэкономической деятельности, организации переговоров, приемов и других совместных с зарубежными специалистами мероприятий на территории предприятия и вне ее.
Оказывает методическую помощь ответственным исполнителям по вопросам обеспечения экономической безопасности при заключении договоров со сторонними организациями.
Участвует в экспертизе материалов, подготовленных к открытой публикации (статьи, доклады, реклама и др.).
Осуществляет организационно-методическое руководство уполномоченными по защите коммерческой тайны в структурных подразделениях. Проводит консультации для

сотрудников предприятия по организационно-правовым вопросам обеспечения экономической безопасности и способам защиты охраняемой информации.
С привлечением специалистов предприятия изучает все виды деятельности подразделений в целях выявления и закрытия возможных каналов утечки охраняемой информации и нанесения экономического ущерба.
Организует служебные расследования по фактам разглашения охраняемой информации, утраты документов или изделий, содержащих такие сведения, нарушений внутриобъектового и пропускного режима предприятия.
Осуществляет связь с правоохранительными и другими государственными органами по вопросам защиты коммерческой тайны и обеспечения экономической безопасности предприятия.

4. СТРУКТУРА

Исходя из задач и функций в СБ предприятия входят:
Подразделение защиты информации
Подразделение технических средств связи и противодействия техническим средствам разведки
Подразделение охраны.
Задачи, функции, права, ответственность структурных звеньев СБ определяются отдельными положениями и должностными инструкциями сотрудников.

Лабораторное занятие №7.
Тема: Организация службы безопасности предприятия

Содержание занятия

Введение
Вопрос 1. Положение о структуре службы безопасности предприятия.
1.1. Общие положения.
1.2. Правовые основы деятельности службы безопасности.
1.3. Основные задачи службы безопасности.
1.4 Общие функции службы безопасности.
1.5. Состав службы безопасности.
1.6. Права, обязанности и ответственность сотрудников службы безопасности.
1.7. Нештатные структуры службы безопасности.
Вопрос 2. Положение о подразделениях.
2.1. Положение об отделе режима и охраны.
2.2. Положение о секторе режима.
2.3. Положение о секторе охраны.
2.4. Положение о специальном отделе.
2.5. Положение о секторе обработки документов с грифом «коммерческая тайна».
2.6. Положение о группе инженерно-технической защиты.
2.7. Положение о группе безопасности внешней деятельности.

Введение.
В условиях формирования общего экономического пространства перед предприятиями особо остро встает задача сохранения коммерческой тайны. Можно сказать определенно: в период становления рынка недобросовестная конкуренция представляет собой серьезную угрозу этому процессу. Стало почти массовым процессом беззастенчивое заимствование интеллектуальной и промышленной собственности (методик, программ, знания и технологии) сотрудниками предприятий, работающими одновременно в кооперативах, малый предприятиях и других коммерческих структурах. К этому следует добавить целенаправленные действия по сманиванию или подкупу рабочих и служащих предприятий конкурента, чтобы завладеть секретами их коммерческой и производственной деятельности.
Современный промышленный шпионаж предполагает использование новейших достижений электроники, непосредственное тайное наблюдение, кражи со взломом, подкуп и шантаж. Речь идет о настоящей «тайной войне». Вот один из показательных примеров, приведенных в статье «Космический товар по минимальным ценам». Американское космическое ведомство весьма заинтересовано в приобретении у России целого ряда образцов космической техники и технологии по ее созданию, которые «в настоящее время предлагаются русскими по минимальным ценам». «Еще несколько лет назад мы намеревались выкрасть кое-что из этого», — заявило одно, пожелавшее остаться неизвестным, должностное лицо администрации США.
Урон американскому бизнесу от краж торговых секретов превышает по их оценкам 4 млрд. долларов ежегодно. То, что в мировой практике именуется промышленным шпионажем, мы даже не можем юридически классифицировать. С переходом на рыночные отношения и условия самостоятельности предприятий перед нами встали серьезные проблемы по обеспечению сохранности своих коммерческих секретов и безопасности предприятия.
Отечественный и зарубежный опыт свидетельствует, что основную роль в обеспечении

сохранности коммерческой тайны играют сами предприятия, а не государственные органы. Для защиты коммерческих секретов предприятия создают собственные службы безопасности. Важной предпосылкой создания службы безопасности предприятия является разработка ее структуры, состава, положений о подразделениях, и должностных инструкций для руководящего состава и сотрудников. Настоящее издание содержит справочный материал для специалистов, занятых разработкой защитных мероприятий, созданием систем безопасности, и для руководителей предприятий, поставивших перед собой задачу обеспечения безопасности производства и коммерческих секретов.

Вопрос 1. Положение о структуре службы безопасности предприятия.

Многогранность сферы обеспечения безопасности и защиты информации требует создания специальной службы, осуществляющей реализацию специальных защитных мероприятий.

Структура, численность и состав службы безопасности предприятия (фирмы, компании и т.д.) за рубежом определяются реальными потребностями предприятия и степенью конфиденциальности ее информации. В зависимости от масштабов и мощности организации деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы компании с развитой штатной численностью. В зарубежных источниках, например, рассматривается следующая структура службы безопасности фирмы (рис. 1). Она возглавляется начальником службы безопасности, которому подчинены служба охраны, инспектор безопасности, консультант по безопасности и служба противопожарной охраны.

С учетом накопленного зарубежного и отечественного опыта и особенностей рыночной экономики предлагается рабочий вариант службы безопасности предприятия среднего масштаба производства, ее структура и должностные инструкции (рис. 2).

1.1. Общие положения.

Основными задачами службы безопасности предприятия являются обеспечение безопасности предприятия, производства, продукции и защита коммерческой, промышленной, финансовой, деловой и другой информации, независимо от ее назначения и форм при всем многообразии возможных каналов ее утечки и различных злонамеренных действий со стороны конкурентов.

1.2. Правовые основы деятельности службы безопасности.

Основные положения, состав и организация службы безопасности имеют юридическую силу в том случае, если они зафиксированы в основополагающих правовых, юридических и организационных документах предприятия.

В основу деятельности службы безопасности положены: Закон Российской Федерации «О безопасности";

Законы и регламенты России, обеспечивающие безопасность деятельности и сохранность коммерческой тайны;

Закон о предприятиях и предпринимательской деятельности; Кодекс законов о труде (КЗОТ);

Устав предприятия, коллективный договор, трудовые договоры, правила внутреннего трудового распорядка сотрудников, должностные обязанности руководителей, специалистов, рабочих и служащих.

1.3. Основные задачи службы безопасности.

Основными задачами службы безопасности предприятия являются: обеспечение безопасности производственно-торговой деятельности и

защиты информации и сведений, являющихся коммерческой тайной; организация работы по правовой, организационной и инженерно-

технической (физической, аппаратной, программной и математической) защите коммерческой тайны;

организация специального делопроизводства, исключающего несанкционированное

получение сведений, являющихся коммерческой тайной;
предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;
обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

1.4 Общие функции службы безопасности.

Служба безопасности предприятия выполняет следующие общие функции:
организует и обеспечивает пропускной и внутри объектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;
руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;
участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны";
изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности предприятия и его клиентов, партнеров, смежников;
организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;
разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие
нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;
осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;
организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был глубоко осознанный подход;
ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

1.5. Состав службы безопасности.

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия.
Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.
Организационно служба безопасности состоит из следующих структурных единиц:
отдела режима и охраны, в составе сектора режима и сектора охраны; специального отдела в составе сектора обработки секретных документов
и сектора обработки документов с грифом «Коммерческая тайна"; инженерно-технической группы;
группы безопасности внешней деятельности.

1.6. Права, обязанности и ответственность сотрудников службы безопасности.

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, имеют право:
требовать от всех сотрудников предприятия, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;
вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.
Сотрудники службы безопасности обязаны:
осуществлять контроль за соблюдением «инструкции по защите коммерческой тайны";
докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действий, могущих привести к утечке конфиденциальной информации или утрате документов или изделий;
не допускать неправомерного ознакомления с документами и материалами с грифом «Коммерческая тайна» посторонних лиц.
Сотрудники службы безопасности несут ответственность за личное нарушение безопасности коммерческой тайны и за не использование своих прав при выполнении функциональных обязанностей по защите конфиденциальных сведений сотрудниками предприятия.

1.7. Нештатные структуры службы безопасности.

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства предприятия и службы безопасности могут создаваться отдельные комиссии, решающие определенные контрольно-ревизионные функции на временной или постоянной основе, такие как:
квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей);
комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т.п.;
периодические проверочные комиссии для проверки знаний и умений выполнять требования нормативных документов по защите коммерческой тайны, а также по оценке эффективности и надежности защитных мероприятий по обеспечению безопасности предприятия.

Вопрос 2. Положение о подразделениях.

Состав и функции подразделений службы безопасности определяются соответствующими Положениями.
Положение о структурном подразделении — документ, предназначенный для

нормативно-правовой регламентации деятельности каждого структурного подразделения. Положение определяет статус подразделения, отражает его место в составе службы безопасности, показывает его внутреннюю организацию. На основе Положения составляется штатное расписание подразделения, определяется степень ответственности за выполнение возложенных на него задач.

2.1. Положение об отделе режима и охраны.

2.1.1. Общие положения.

Отдел режима и охраны является самостоятельным структурным подразделением службы безопасности и подчиняется начальнику службы безопасности.

В своей деятельности отдел руководствуется требованиями «Инструкции по организации режима и охране».

2.1.2. Задачи.

Организация и осуществление мер по обеспечению безопасности деятельности и защите сведений, составляющих государственную и коммерческую тайну.

Разработка и совершенствование системы предотвращения несанкционированного допуска и доступа к сведениям, составляющим коммерческую тайну.

Организация и поддержание пропускного и внутри объектного режима.

Организация охраны арестованных по режиму конфиденциальных помещений.

Организация личной охраны руководителей и ведущих сотрудников.

Организация и установление мер физической и технической защиты зданий и помещений.

Организация, разработка и контроль системы безопасности в повседневных и в особых условиях (стихийные бедствия, поломки, аварии, беспорядки и т.п.).

2.1.3. Структура.

В составе отдела режима и охраны имеются следующие структурные единицы:

Сектор режима.

Сектор охраны.

2.1.4. Функции.

В соответствии с основными задачами отдел режима и охраны выполняет следующие функции:

Организует работу по выполнению решений, приказов и распоряжений руководства предприятия по обеспечению защиты коммерческих секретов и обеспечению безопасности деятельности.

Определяет единство действий и организует защиту, безопасность, сохранность документов и ценностей в обычных и особых условиях.

Разрабатывает, обновляет и дополняет инструкции, положения и иные нормативные материалы по режиму и охране.

Осуществляет руководство работой по установлению степени конфиденциальности сведений, содержащихся в документах. Совместно с основными подразделениями проводит работу по анализу практики применения «Перечня сведений, составляющих коммерческую тайну», по подготовке и внесению в него в установленном порядке необходимых изменений и дополнений, а также организует его переработку и переиздание.

Организует разработку и контроль за эффективностью действующей разрешительной системы допуска сотрудников, компаньонов и клиентов к ознакомлению и работе с документами конфиденциального характера, с целью исключения возможности ознакомления со сведениями, не относящимися к выполняемой ими работе.

Разрабатывает и рассматривает совместно со специальным отделом и подразделениями предложения по совершенствованию делопроизводства с грифом «Коммерческая тайна», предотвращению факторов включения в документы секретного и несекретного характера излишнего объема сведений, являющихся коммерческой тайной, сокращению издаваемых и разрабатываемых документов конфиденциального характера, неоправданной из

рассылки.
Организует и обеспечивает систему контролируемого доступа и специального пропускного режима в здания и помещения.
Организует, обеспечивает и контролирует выполнение требований внутри объектного режима.
Определяет систему охраны и участвует в ее организации и обеспечении работы выделенных помещений.
Организует разработку тактических принципов использования средств автоматизации, сигнализации, связи и охраны.
Организует охрану, пропускной, допускной и внутри объектный режим и осуществляет оперативно-методическое руководство работами по защите выделенных помещений и информации, обрабатываемой и передаваемой с использованием технических средств.
Осуществляет руководство и режим защиты коммерческих сведений в работе по отбору, хранению и использованию архивных материалов.
Осуществляет методическое руководство и принимает непосредственное участие в проведении предупредительно-профилактической работы с исполнителями работ и документов конфиденциального характера.
Организует проведение служебных расследований по фактам утраты документов конфиденциального характера, разглашения охраняемых сведений, нарушения охраны и пропускного режима, необоснованного ознакомления сотрудников и командированных лиц со сведениями, составляющими государственную и коммерческую тайну и по другим фактам, которые привели или создавали условия, способствующие утечке конфиденциальной информации.
Обеспечивает личную охрану руководства и сотрудников.

2.1.5. Права начальника отдела.

На основе единоличия руководит деятельностью отдела режима и охраны по выполнению возложенных на отдел задач и функций.
Назначает проведение проверок состояния и эффективности работы по обеспечению сохранения коммерческих секретов, режима безопасности, охраны и технического ее обеспечения.
Требует от сотрудников представления объяснений по фактам, которые привели или могли привести к утечке информации, составляющей коммерческую тайну.
Ходатайствует о поощрении сотрудников, активно участвующих в работе по предупреждению утечки охраняемых сведений, выполнении требований режима и охраны.

2.2. Положение о секторе режима.

2.2.1. Общие положения.

Сектор режима является подразделением отдела режима и охраны службы безопасности и подчиняется непосредственно начальнику отдела.
В своей деятельности сектор руководствуется требованиями «Инструкции по режиму и охране» в части режима.

2.2.2. Задачи.

Организация пропускного и внутри объектного режима.
Разработка разрешительной системы и обеспечение допуска сотрудников к документам, материалам и сведениям, составляющим коммерческую тайну.
Контроль за соблюдением режима допуска к сведениям и документам.
Совершенствование системы пропускного и внутри объектного режима.
Участие в разработке «Перечня сведений, составляющих коммерческую тайну».

2.2.3. Структура.

В составе сектора режима выделяются следующие штатные должности: заведующий сектором режима;
старший инспектор по режиму — начальник бюро пропусков; инспектор по режиму;

инспектор по работе с персоналом, допущенным к сведениям, составляющим коммерческую тайну.

2.2.4. Функции.

В части обеспечения режима основными функциями сектора являются разработка, реализация и осуществление основных положений системы получения разрешений на доступ к информации, составляющей коммерческую тайну, в том числе:

права, обязанности и ответственность сотрудников, допущенных к работе с документами, содержащими коммерческую тайну;

схема выдачи разрешений на доступ сотрудников к сведениям, составляющим коммерческую тайну;

порядок доступа на совещания по вопросам, содержащим сведения, составляющие коммерческую тайну;

порядок и контроль доступа к сведениям, составляющим коммерческую тайну, представителей других предприятий и государственных органов;

ведение, уточнение и изменение «Перечня сведений, составляющих коммерческую тайну";

учет сотрудников, допущенных к работе с документами и материалами, содержащими сведения, составляющие коммерческую тайну;

учет и анализ нарушений режима работы с документами, содержащими коммерческую тайну, различного рода попыток несанкционированного доступа к конфиденциальным документам традиционного и автоматизированного исполнения (базы данных, персональные файлы и др.), случаев телефонных переговоров, содержащих конфиденциальную информацию;

организация и проведение деловых совещаний, переговоров и встреч с обсуждением вопросов, связанных с коммерческой тайной;

организация и обеспечение пропускного и внутри объектного режима: выдача пропусков (постоянных, временных, разовых), порядок посещения, учет посетителей;

определение выделенных помещений, проведение их паспортизации, обеспечение их защиты совместно с группой Инженерно-технической защиты информации.

В части работы с персоналом учитывается, что сотрудники — главный источник утечки конфиденциальной информации. С учетом этого функции группы составляют:

беседы с поступающими на работу в подразделения, работа которых связанна с коммерческой тайной, с целью установления их пригодности для этой работы;

изучение поступающего на работу в части его прошлой трудовой деятельности;

оформление обязательств о неразглашении сведений, составляющих коммерческую тайну;

анализ служебной осведомленности сотрудников;

анализ и учет трудовой удовлетворенности с целью предупреждения увольнения сотрудников, допущенных к сведениям, составляющим коммерческую тайну;

ведение досье на сотрудников, допущенных к документам с коммерческой тайной;

организация обучения сотрудников по вопросам защиты коммерческой тайны;

беседы с увольняющимися и оформление контракта (обязательства) не разглашать коммерческие секреты.

Кроме того, сектор в тесном взаимодействии с отделом кадров: разрабатывает планы комплектования кадрами;

оформляет прием, перевод и увольнение сотрудников, допущенных к коммерческой тайне;

готовит материалы для преставления сотрудников к поощрениям и должностным перемещениям.

2.2.5. Права.

Проводить беседы с поступающими на работу и увольняющимися и оформлять обязательства не разглашать коммерческие секреты.

Требовать от сотрудников и клиентов строгого выполнения установленного пропускного

и внутриобъектового режима;
Проводить проверку состояния и организации работы по обеспечению режима работы с документами составляющими коммерческую тайну.
Требовать от сотрудников письменных объяснений по фактам нарушения пропускного и внутриобъектового режима;
Возбуждать ходатайства перед руководством о привлечении к дисциплинарной ответственности лиц, допустивших нарушения режима.
Представлять к поощрениям сотрудников, добросовестно выполняющих обязанности по сохранению в тайне охраняемых сведений.

2.2.6. Ответственность.

Всю полноту ответственности за выполнение задач и функций по режиму и работе с персоналом несет заведующий сектором режима.
Степень ответственности других сотрудников сектора устанавливается должностными инструкциями.

2.3. Положение о секторе охраны.

2.3.1. Общие положения.

Сектор охраны является подразделением отдела режима и охраны службы безопасности и подчиняется непосредственно начальнику отдела.
В своей деятельности сектор руководствуется требованиями «Инструкции по режиму и охране» в части охраны.

2.3.2. Задачи.

Обеспечение надежной защиты зданий, помещений, оборудования, валютных и материальных ценностей, а также личной охраны руководящего состава в обычных и экстремальных условиях.

2.3.3. Структура.

Сектор охраны состоит из:
комендантской службы;
группы личной охраны руководства.
Комендантская служба может состоять из коменданта здания, дежурного мастера по вневедомственной и объектовой технической охране и дежурного мастера по противопожарной охране.

2.3.4. Функции.

Сектор охраны осуществляет охрану зданий, помещений, оборудования, линий связи и перевозок, пожарную охрану, а также личную охрану руководящего состава.
Сектор охраны обеспечивает необходимые условия, исключающие несанкционированный доступ в охраняемые здания, помещения, отдельные конфиденциальные участки и зоны территории и служебных помещений. Особое внимание уделяется критическим условиям, связанным со стихийными бедствиями, поломками, авариями.
Сектор охраны:
реализует учет, контроль и наблюдение за охраняемыми зонами, помещениями, хранилищами;
обеспечивает установку и работу на местах технических средств охраны, охранной и пожарной сигнализации;
осуществляет прием под охрану и сдачу в эксплуатацию охраняемых помещений, проверяя при этом надежное срабатывание средств охраны, делая соответствующую запись в журнале приема и сдачи под охрану;
принимает меры по ликвидации возможных пожаров и других аварийных ситуаций.
В части личной охраны руководящего состава сектор руководствуется отдельным положением, разрабатываемым службой безопасности с учетом конкретных условий ее деятельности.

2.3.5. Права.

Проверять наличие, состояние и функционирование технических средств охраны

охранной и пожарной сигнализации.
Требовать строгого соблюдения установленного внутриобъектового режима и правил трудового распорядка
Участвовать в разработке мероприятий по усилению безопасности и сохранности имущества, средств, зданий и помещений.
Не допускать случаев использования неисправного оборудования, охранной и пожарной техники.
Принимать меры воздействия к сотрудникам, допускающим порчу или неправильную эксплуатацию охранно-пожарной техники.
Требовать своевременного ремонта и профилактики технических средств охраны и пожарной сигнализации.

2.3.6. Ответственность.

Всю полноту ответственности за качество и своевременное выполнение возложенных на сектор настоящим Положением задач и функций несет заведующий сектором.

2.4. Положение о специальном отделе.

2.4.1. общие положения.

Специальный отдел является самостоятельным структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.
В своей деятельности отдел руководствуется требованиями «Инструкции по режиму и охране» в части коммерческих секретов.

2.4.2. Задачи.

Организация и руководство делопроизводством секретных документов и документов с грифом «Коммерческая тайна».

2.4.3. Структура.

Специальный отдел состоит из следующих структурных единиц: сектор обработки секретных документов;
сектор обработки документов с грифом «Коммерческая тайна"; машинописное бюро оформления специальных документов; экспедиция.

2.4.4. Функции.

Обработка поступающей и отправляемой корреспонденции, доставка ее по назначению.
Осуществление контроля за сроками исполнения документов.
Организация работы по регистрации, учету и хранению документальных материалов текущего пользования.
Разработка номенклатуры дел, осуществление контроля за правильным формированием дел в подразделениях и подготовкой материалов к своевременной сдаче в архив.
Разработка и внедрение предложений по совершенствованию системы делопроизводства.
Печатание и размножение секретных документов и документов с грифом
«Коммерческая тайна».
Участие в подготовке созываемых и проводимых руководством закрытых совещаний и организация их технического обслуживания.
Специальный отдел в части обеспечения обработки секретных документов руководствуется соответствующими документами, в части ведения делопроизводства с грифом «Коммерческая тайна» выполняет требование «Инструкции по защите коммерческой тайны».

2.4.5. Права.

Требовать от руководителей подразделений и исполнителей четкого и своевременного выполнения нормативных документов по организации и ведению специального делопроизводства.
Регулярно проверять правильность ведения делопроизводства в подразделениях, указывать руководителям подразделений на выявленные недостатки и требовать их устранения.

Возвращать исполнителям документы, оформленные с нарушением установленных правил делопроизводства.
Указания специального отдела в пределах его функций, предусмотренных Положением, являются обязательными к руководству и исполнению подразделениями предприятия.

2.4.6. Ответственность.

Всю полноту ответственности за качество и своевременное выполнение возложенных настоящим Положением задач и функций несет заведующий отделом.
Степень ответственности других сотрудников отдела устанавливается должностными инструкциями.

2.5. Положение о секторе обработки документов с грифом «коммерческая тайна».

2.5.1. Общие положения.

Сектор обработки документов с грифом «Коммерческая тайна» является структурным подразделением специального отдела службы безопасности и подчиняется непосредственно заведующему отделом. В своей работе сектор руководствуется «Инструкцией по защите коммерческой тайны».

2.5.2. Задачи.

Организация и руководство делопроизводством документов с грифом «Коммерческая тайна».

2.5.3. Структура.

В составе вектора устанавливаются следующие должности: заведующий сектором; делопроизводитель; машинистка.

2.5.4. Функции.

Получение, учет, исполнение и документирование поступающих и разрабатываемых документов, организация оптимального документооборота, обеспечение отправки, размножения и надежного хранения документов, их сохранности и своевременного уничтожения, а также проверка их наличия и контроль своевременного и правильного их исполнения.
Разработка нормативных документов, направленных на обеспечение сохранности коммерческой тайны.
Участие в разработке, пополнении и обновлении «Перечня сведений, составляющих коммерческую тайну».
Участие в процессе обучения персонала работе с документами, содержащими коммерческую тайну.

2.5.5. Права.

Требовать от подразделений, руководителей, сотрудников соблюдения требования по ведению делопроизводства с грифом «Коммерческая тайна».
Проверять правильность ведения делопроизводства в подразделениях, указывать руководителям подразделений на выявленные недостатки и требовать их устранения.
Представлять к поощрению сотрудников, четко выполняющих требования по сохранению коммерческой тайны. Принимать меры воздействия к лицам, допускающим нарушения в работе с документами, содержащими сведения, составляющие коммерческую тайну.

2.5.6. Ответственность.

Всю полноту ответственности за качество и своевременное выполнение возложенных настоящим Положением на сектор задач и функций несет заведующий сектором.
Степень ответственности других сотрудников сектора устанавливается должностными инструкциями.

2.6. Положение о группе иженерно-технической защиты.

2.6.1. Общие положения.

Группа инженерно-технической защиты информации является структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.

В своей деятельности группа руководствуется требованиями «Инструкции по Инженерно-технической защите».

2.6.2. Задачи.

Обследование выделенных помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации через технические средства, конструкции зданий и оборудования.

Выявление и оценка степени опасности технических каналов утечки информации.

Разработка мероприятий по ликвидации (локализации) установленных каналов утечки информации организационными, организационно- техническими или техническими мерами, используя для этого физические, аппаратные и программные средства и математические методы защиты.

Организация контроля (в том числе и инструментального) за эффективностью принятых защитных мероприятий. Проведение обобщения и анализа результатов контроля и разработка предложений по повышению надежности и эффективности мер защиты.

Обеспечение приобретения, установки, эксплуатации и контроля состояния технических средств защиты информации.

2.6.3. Структура.

Структура и штатный состав группы Инженерно-технической защиты информации разрабатывается и утверждается руководством службы безопасности исходя из конкретных условий и технической оснащенности подразделений предприятия.

Возможно состав группы установить в следующем составе: руководитель группы — старший инженер;

Инженер (техник) группы по спец измерениям.

2.6.4. Функции.

Определение границ охраняемой (контролируемой) территории (зоны) с учетом возможностей технических средств, наблюдения злоумышленников.

Определение технических средств, используемых для передачи, приема и обработки конфиденциальной информации в пределах охраняемой территории (зоны).

Определение опасных, с точки зрения возможности образования каналов утечки, технических средств.

Локализация возможных каналов утечки информационно- организационными, организационно-техническими или техническими средствами и мероприятиями.

Организация наблюдения за возможным неконтролируемым излучением за счет ПЭМИН (побочных электромагнитных излучений и наводок).

Организация контроля наличия, проноса каких-либо предметов (устройств, средств, механизмов) в контролируемую зону, способных представлять собой технические средства несанкционированного получения конфиденциальной информации.

2.6.5. Права.

Группа Инженерно-технической защиты информации имеет право: проверять наличие технических средств обеспечения производственной

Деятельности в выделенных помещениях, измерять их параметры на соответствие требованиям безопасности;

устанавливать технические средства защиты каналов утечки информации через технические средства обеспечения производственной деятельности;

запрещать использование технических средств, не обеспечивающих требования безопасности.

2.6.6. Ответственность.

Всю полноту ответственности за инженерно-техническую защиту информации несет руководитель группы.

2.7. Положение о группе безопасности внешней деятельности.

2.7.1. Общие положения.

Группа безопасности внешней деятельности является самостоятельным структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.

Группа организует работу в тесном взаимодействии с основными структурными подразделениями службы безопасности и предприятия.

2.7.2. Задачи.

Изучение и выявление предприятий и организаций, потенциально являющихся союзниками и конкурентами.

Добывание, сбор и обработка сведений о деятельности потенциальных и реальных конкурентов для выявления возможных злонамеренных действий по добыванию охраняемых сведений.

Учет и анализ попыток несанкционированного получения коммерческих секретов конкурентами.

Оценка степени реальных конкурентных отношений между сотрудничающими (конкурирующими) организациями.

Анализ возможных каналов утечки конфиденциальной информации.

2.7.3. Структура. Структура и штатное расписание определяется с учетом объемов и особенностей обстановки.

2.7.4. Функции.

Изучение торгово-конъюнктурных ситуаций в пространстве деятельности учредителей, партнеров, клиентов и потенциально возможных конкурентов.

Ситуационный анализ текущего состояния финансово-торговой деятельности с точки зрения прогнозирования возможных последствий, могущих привести к неправомерным действиям со стороны конкурирующих организаций и предприятий.

Выявление платежеспособности юридических и физических лиц, их возможности по своевременному выполнению платежных обязательств.

Установление антагонистических конкурентов, выявление их методов ведения конкурентной борьбы и способов достижения своих целей.

Определение возможных направлений и характера злоумышленных действий со стороны специальных служб промышленного шпионажа против предприятия, его партнеров и клиентов.

2.7.5. Права.

Требовать от соответствующих служб и подразделений необходимые для анализа сведения о деятельности партнеров и клиентов.

Осуществлять сбор и обработку необходимых сведений для выявления злоумышленных действий со стороны конкурирующих организаций.

2.7.6. Ответственность.

Вся полнота ответственности за полноту и своевременность оценки степени опасности действий со стороны конкурентов и злоумышленников по отношению к охраняемым сведениям и безопасности руководства и сотрудников лежит на группе безопасности внешней деятельности.

Лабораторное занятие №8.
Тема: Системный подход к разработке концепции обеспечения безопасности информационного объекта

СОДЕРЖАНИЕ ЗАНЯТИЯ

Обеспечение безопасности объектов (важных, особо важных, особого риска, режимных, особо режимных, не режимных, но содержащих значительные материальные ценности и т.д.) представляет собой столь широкую и многогранную область деятельности, что она в той или иной мере осуществляется практически многими предприятиями и организациями других министерств и ведомств самостоятельно, сообразуя с характерными или специфическими только для этих предприятий и организаций условиями деятельности, например: Федеральная служба безопасности, Министерство обороны, Министерство внутренних дел, Министерство по связи и информатизации и т.д.
Основными направлениями деятельности СБ (О) по обеспечению комплексной безопасности (в части, не касающейся пожарной безопасности) являются:

- инженерная и техническая защита территорий, зданий и помещений;
- организация контроля доступа сотрудников и командированных (посетителей);
- организация охраны особо важных помещений (жизненно важных центров);
- создание систем охранной сигнализации и телевизионного наблюдения;
- разработка рекомендаций по режиму охраны объектов и выработка предложений по работе СБ (О);
- защита объектов от угроз утечки информации, создание защищенных зон;
- контроль проноса технических средств в особо важные помещения (жизненно важные центры);
- выявление закладных средств подслушивания и видеонаблюдения в помещениях;
- проверка технических устройств обработки информации на наличие каналов утечки и разработка рекомендаций по их защите;
- организация непрерывного технического контроля опасных сигналов в каналах утечки;
- защита объектов от применения диверсионно - террористических средств;
- обеспечение безопасности автоматизированных систем обработки информации от несанкционированного доступа (НСД), несанкционированного копирования (ИСК), вирусной диверсии и других угроз;
- обеспечение применения специальных технических средств контроля особо важных помещений;
- организация контроля телефонных переговоров с их регистрацией.

Создание надежной системы защиты ДТА предполагает реализацию определенного типового порядка при проведении специальных работ, как то:

- анализ объекта и условий его расположения;
- рассмотрение возможных угроз воздействия на объект;
- специальный анализ ситуации для строящихся и реконструируемых объектов;
- разработка концепции безопасности от всех видов негативных воздействий;
- выработка предложений по техническому оснащению средствами безопасности на основе разработанной концепции и разработка проекта на оборудование инженерно-техническими и специальными средствами;
- приобретение и монтаж специальных технических средств и комплексов (в соответствии с разработанным проектом);
- обучение персонала приемам и способам использования специальных технических

средств, постоянный контроль за эксплуатацией поставленных средств.
Ряд блоков задач может быть реализован на основе определенной типизации, исходя (опять-таки) из анализа параметров, характеризующих объект, условий его функционирования, потенциальных угроз, объема и свойств имеющихся (хранимых) энергоемких материалов и т.д. В каждом случае должна быть осуществлена классификация по структуре, качеству и свойствам применяемых технических средств защиты. Таким путем конкретизируется вопрос разработки рациональных схем защиты по каждому блоку задач на основе выбора конкретных технических средств из предлагаемых на рынке.
Пример. Для решения задач оборудования периметра какого-либо объекта техническими средствами охранной сигнализации предварительно следует знать ответы на вопросы:

1. Какова протяженность периметра.
2. Вид имеющегося заграждения (его параметры, материал).
3. Количество имеющихся ворот, калиток, их размеры, материал.
4. Ближайшее расстояние от охраняемого рубежа до помещения охраны, до ближайшего к периметру здания.
5. Наличие закладных (трубы, кабели).
6. Размер зоны отчуждения внутри периметра, наличие кустов и/или деревьев в зоне отчуждения.
7. Необходимость скрытности средств обнаружения (или отсутствие такой необходимости).
8. Требуемая точность обнаружения нарушителя на контуре периметра (3м, 10м, ...).
9. Требуемое количество рубежей охраны (периметр, подходы к зданиям), режимы охраны: круглосуточный, по мере необходимости, М-часовой.
10. Необходимость блокирования: перелаза через ограждения, разрушения ограждения, подкопа под ограждения.

Примечание. Здесь рассматривается лишь модель физического проникновения. Если же требуется информационная защита - задача охраны многократно усложняется.

11. Наличие в настоящее время (т.е. на момент предварительного анализа объекта охраны) каких-либо средств обнаружения, станционной аппаратуры в помещении службы охраны - системы сбора и обработки информации.
12. Какие затраты может позволить себе Заказчик на решение задач оборудования объекта (в частности периметра) техническими средствами охранной сигнализации и системой сбора и обработки информации.
13. В какие сроки требуется проведение такой работы. 14.Необходимы план объекта (эскиз), параметры по высоте зданий.

Примечания.

- Следует описать пожелания службы охраны (реальные с позиций затрат) для выбора ТСОС и ССОИ.
- Уровень полноты решения задач7,8,9,10 существенно влияет на размеры затрат.

Приведенный перечень вопросов - минимально необходимый с позиций предварительного анализа, но далеко не полный с позиций системного подхода.
Объективная необходимость построения высоко эффективных систем безопасности объектов в условиях резкого обострения криминогенной обстановки привела к разработке наукоемких интегрированных систем безопасности (ИСБ). ИСБ по существу нацелена на реализацию идей системной концепции обеспечения комплексной безопасности объекта с параллельным (интегрированным с задачами обеспечения безопасности) решением задач автоматизации управления широкой гаммой систем жизнеобеспечения объекта, как то: энергоснабжением, вентиляцией, отоплением, водоснабжением, лифтовым оборудованием, кондиционированием и т.д.

Среди функций, обязательных для исполнения в контуре ИСБ, следует считать:

- контроль за большим количеством помещений с созданием нескольких рубежей защиты (ИСБ разрабатывается только для больших объектов и зданий);
- иерархический доступ сотрудников и посетителей в помещения с четким разграничением полномочий по праву доступа в помещения по времени суток и по дням недели;
- идентификацию и аутентификацию личности человека, пересекающего рубеж контроля;
- предупреждение утечки информации;
- предупреждение попадания на объект запрещенных материалов и оборудования;
- накопление документальных материалов для использования их при рассмотрении и анализе происшествий;
- оперативный (автоматизированный) инструктаж работников охраны о порядке действий в различных штатных и нештатных ситуациях путем автоматического вывода на экран монитора инструкций в нужный момент;
- обеспечение полной интеграции систем видеонаблюдения, сигнализации, мониторинга доступа, оповещения, связи между персоналом СБ (О), персоналом службы пожарной безопасности, персоналом служб жизнеобеспечения объекта и т.д.;
- обеспечение взаимодействия постов охраны и органов правопорядка при несении охраны и в случае происшествий;
- слежение за точным исполнением персоналом охраны своих служебных обязанностей.

Исходя из изложенного ранее ясно, что составными частями ИСБ (укрупненно) должны быть:

- сеть датчиков, обеспечивающих получение максимально полной информации со всего пространства, находящегося в поле зрения службы безопасности и позволяющая воссоздавать на центральном пульте наблюдения и управления всестороннюю объективную картину состояния помещений, всей территории объекта и работоспособности всей аппаратуры и оборудования, включенного в контур ИСБ;
- исполнительные устройства, способные при необходимости действовать автоматически или по команде оператора;
- пункты контроля и управления системой отображения информации, через которые операторы могут следить за работой всей системы в пределах своих полномочий;
- ССОИ, наглядно представляющая информацию с датчиков и накапливающая ее для последующей обработки;
- коммуникации, по которым осуществляется обмен информацией между элементами системы и операторами.

При этом важно наличие возможности оперативного программирования (перепрограммирования) функций ИСБ. Это позволяет противодействовать эффективно таким ухищрениям злоумышленника как:

1. Исходные положения для разработки системной концепции обеспечения безопасности объектов охраны

В данном разделе излагаются основные направления деятельности по обеспечению безопасности объектов охраны (ОО), привлекательных для преступников с различных точек зрения. Преступные посягательства могут преследовать различные цели, например:

- кражи материальных и/или информационных ценностей;
- имеющие в своей основе террористические действия, направленные на решение политических или грабительских задач, как то: разрушение объекта (вывод его из строя); захват управления функционированием объекта (например, если это объекты

радиовещания, телевидения, связи, то захват осуществляется для решения задач дезинформации, пропаганды, информационной блокады населения); информационная разведка; ограбление; внедрение членов организованных преступных формирований (ОФП) или групп (ОПГ) в управленческие структуры и т.д.

Актуальность системного решения проблем и задач охранной деятельности особенно возросла в последние годы, что диктуется многими факторами, например:

- в современных условиях становления новых общественных, экономических, политических, производственных и иных отношений при недостатке механизмов их правового регулирования происходит закономерный взрыв криминогенной обстановки. Резко активизируется деятельность организованных преступных структур, происходит их количественный рост, качественная техническая и методическая оснащенность, проникновение в коммерческие, государственные, в том числе и в правоохранительные органы. По информационно- аналитическим обзорам специалистов (экспертов) уровень преступности в ближайшие годы будет сохраняться;
- преступные действия организованных структур, направленные на захват и ограбление учреждений, на получение конфиденциальной (секретной) информации о деятельности предприятий и т.д., все в большей степени подготавливаются как глубоко продуманные, технически хорошо оснащенные, смоделированные на достаточно высоком интеллектуальном и психологическом уровне акции;
- по данным экспертов подготовка и проведение преступных акций в большинстве случаев осуществляются на высоком профессиональном уровне, характеризуются системным решением (в том числе и в плане сокрытия следов) и часто отличаются жестокостью исполнения.

Исходя из изложенного, разработчики системной концепции обеспечения безопасности объектов в максимальной степени должны учитывать мировой и отечественный опыт, касающийся всей многогранной деятельности, организуемой по защите объектов.

Практика охранной деятельности показывает что необходим научнообоснованный подход к решению проблем и задач охраны объектов, в особенности, если это особо важные, особо опасные объекты, объекты особого риска или объекты, содержащие большие материальные ценности (например, банки, хранилища драгоценных камней и металлов и т.д.).

В связи с тем, что наиболее высоким уровнем разработки систем защиты характеризуются особо опасные, особо важные, особо режимные объекты и банки, и этот опыт, безусловно, полезен для объектов многих отраслей
народного хозяйства, где возможно придется работать сегодняшним студентам, в списке литературы приведены наименования соответствующих источников, опубликованных в открытой печати.

Очевидно, коль скоро действия преступников часто носят не просто ухищренный, а системно продуманный профессионалами характер, им следует противопоставить организацию и оснащение, выполненные на более высоком уровне профессионализма. Этим и объясняется необходимость разработки обобщенной системной концепции по обеспечению безопасности объектов, которая в каждом случае должна быть адаптирована к конкретному объекту, исходя из условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и обстановки и т.д. Таким образом, для каждого конкретного объекта должна разрабатываться на основе общей своя собственная концепция безопасности, исходя из положений которой разрабатывается проект оснащения объекта инженерно-техническими, специальными и программно-аппаратными средствами защиты.

Технические средства охраны (ТОО), установленные на объектах охраны, должны в комплексе с силами физической охраны и системой инженерных сооружений удовлетворять современным (исходя из сложившейся криминогенной обстановки) требованиям по охране ОО от устремлений потенциального нарушителя.

Учитывая изложенное, разработчики технических средств охранной сигнализации (ТСОС) и комплексов технических средств охраны (КТСО) при анализе исходных положений для определения "моделей нарушителей" должны рассматривать и такие факторы, характерные для современной жизни, как:

- наличие в свободной продаже зарубежных и отечественных изделий спецтехники;
- возможность приобретения современного вооружения;
- возможность рекрутирования организованными преступными формированиями подготовленных в силовых структурах людей;
- наличие значительных финансовых ресурсов в криминальных структурах и т.д., т.е. факторов, расширяющих возможность преступных формирований организовывать против объектов охраны преступные действия с высоким уровнем их предварительной подготовки.

Одной из центральных подсистем в системе обеспечения безопасности ОО является автоматизированная система охраны (АСО), с помощью которой реализуются практические меры по предупреждению недозволенного доступа к технике, оборудованию, материалам, документам и охране их от шпионажа в пользу конкурентов, диверсий, повреждений, хищений и других незаконных или преступных действий.

На практике действия АСО (рис. 1) складываются из двух основных фаз: обнаружение нарушителя (в возможно короткий период времени с момента его появления в охраняемой зоне) и его задержание.

Задачи обнаружения нарушителя и определения места его проникновения могут быть решены как с помощью патрулей из личного состава службы охраны, так и с помощью технических средств охраны. Задачи обнаружения нарушителя и контроля за состоянием безопасности охраняемых объектов решаются, главным образом, с помощью технических средств охраны и телевизионного наблюдения. Применение этих средств позволяет в разумных пределах (с точки зрения реализации определенной тактики охраны) снизить численность личного состава охраны, но при этом повысить надежность защиты объекта, увеличить оперативность в принятии мер к задержанию нарушителя.

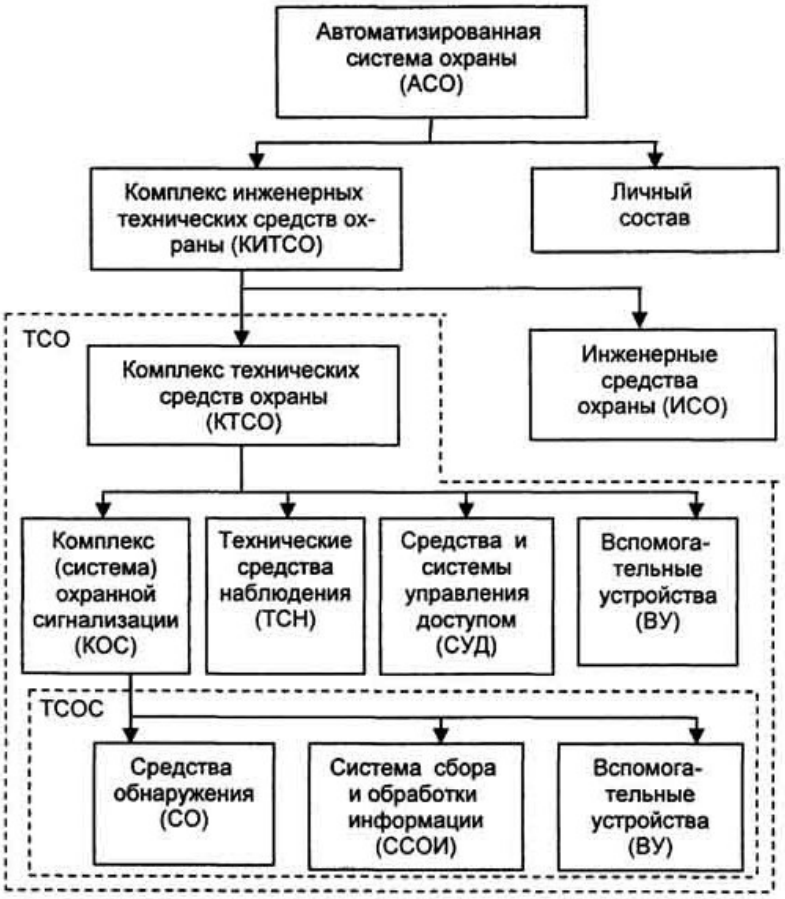


Рис. 1. Структура автоматизированной системы охраны

В общем случае **в состав комплекса технических средств обеспечения безопасности объекта входят:** технические средства охранной сигнализации (ТСОС); технические средства наблюдения (ТСН); система контроля доступа (СКД), в литературе применяются также понятия-синонимы - система управления доступом (СУД) и система контроля и управления доступом (СКУД); технические средства пожарной сигнализации (вопросы пожарной безопасности здесь не рассматриваются); технические средства обнаружения диверсионно-террористических средств и технические средства обнаружения (предотвращения) утечки информации. В состав ТСОС входят: средства обнаружения (СО); система сбора, обработки, отображения и документирования информации (ССОИ); вспомогательные устройства (ВУ) - системы электропитания, охранного освещения, оповещения и т.д.

Для решения задач и проблем выбора структуры и состава комплекса технических средств охраны необходимо, во-первых, проанализировать возможные варианты действий злоумышленника. Далее, для определенности, будем применять термин "нарушитель", имея в виду кого угодно, несанкционированным образом проникающего на охраняемую территорию и в его помещения, а именно: случайного, не имеющего определенных целей, человека; вора; грабителя; террориста или группы людей, вторгающихся с преступной целью. Исходя из анализа возможных действий нарушителя, составляются варианты его моделей, которые и принимаются за основополагающий фактор выбора тактики защиты объекта. Во-вторых, более углубленный или менее углубленный учет параметров моделей нарушителей осуществляется, исходя из значимости, ценности, важности объекта, т.е. требуемой категории его защиты (безопасности).

Важное влияние на оценку параметров нарушителя оказывают его стартовые позиции. Условно их можно разделить на четыре группы:

- нарушитель не имеет доступа на территорию объекта и, соответственно, преодолевает все рубежи охраны;

- нарушитель имеет доступ на объект, но не имеет доступа в режимную зону;
- нарушитель имеет доступ на объект и режимную зону, но не имеет доступа к конкретным охраняемым сведениям или материальным ценностям;
- нарушитель имеет доступ на объект, в режимную зону и к конкретным охраняемым сведениям или материальным ценностям.

Следует отметить, что при более простой (сложной) структуре объекта число стартовых позиций соответственно может уменьшаться (увеличиваться).

Очевидно, что для первой группы вероятность обнаружения и сложность проникновения на объект для совершения противоправных деяний в основном определяется КТСО, а для четвертой -уровнем всей системы обеспечения безопасности, включая и состояние режимной и кадровой работы, проводимой на объекте.

По каждой из возможных угроз необходимо определять территории, подлежащие контролю, и временные интервалы их контроля.

Структурную схему передачи оператору КТСО информации о наличии нарушителя можно представить в виде, приведенном на рис. 2.

Рис. 2. Структурная схема передачи информации о наличии нарушителя

Наиболее опасным, с точки зрения службы безопасности (охраны) объекта (СБ (О)) является подготовленный и технически оснащенный нарушитель, способный применить для обхода ТСОС множество способов. Очевидно, модель защиты должна строиться, исходя из моделирования всех возможных действий злоумышленника.

Вероятность обезвреживания (обнаружения и задержания) нарушителя силами физической охраны существенно зависит от характеристик ТСОС. Первая фаза обнаружение нарушителя - определяется вероятностью обнаружения нарушителя ТСОС, периодом наработки на отказ и временем восстановления ТСОС; вторая фаза - задержание нарушителя - зависит от времени обнаружения нарушителя техническими средствами охранной сигнализации с момента его появления на объекте и периода наработки на ложное срабатывание. Последнее объясняется тем, что при ложном срабатывании силы физической охраны отвлекаются на время проверки сигнала "Тревога" и не способны провести проверку двух и более фактов обработки ТСОС одновременно. Кроме того, ложное срабатывание создает с неизбежностью (объективно по законам психологии) стрессовую ситуацию, снижающую боеготовность сотрудников сил физической охраны на некоторый период времени, необходимый для восстановления гормонального баланса человеческого организма, а также порождает снижение бдительности из-за привыкания к факту появления ложных срабатываний.

Таким образом, при разработке проекта оборудования ОО техническими средствами охранной сигнализации помимо гаммы технических факторов необходимо учитывать факторы, определяемые поведением нарушителя.

Рассмотрим, какие требования к проекту оборудования объекта ТСОС порождаются возможными действиями нарушителя.

Возможность нарушителя найти маршрут, не блокированный СО, должна быть

исключена. Для предотвращения прохода нарушителя должны быть блокированы все возможные маршруты движения нарушителя. Состояние физических преград (инженерных сооружений), имеющих большую стойкость и в связи с этим не блокированных СО, должно периодически контролироваться патрулями из личного состава охраны (обходно-дозорной службы) либо - с использованием телевизионных средств наблюдения.

Для увеличения вероятности обнаружения подготовленного и технически оснащенного нарушителя комплексом технических средств охраны объекта могут организовываться полностью скрытные (маскируемые) рубежи охраны.

С целью повышения устойчивости рубежей охраны к преодолению они должны оборудоваться СО, работающими на разных физических принципах действия (радиоволновые, ИК, сейсмические и т.д.), а также должна быть реализована функция дистанционного контроля. Комбинирование данных СО должно производиться по схеме М из N (например, при М=2, N=3, если сработали не менее двух из трех установленных СО, то принимается решение о выдаче сигнала "Тревога"). Числа М и N определяются в ходе проектирования КТСО индивидуально для каждого рубежа охраны объекта.

Для предотвращения обхода нарушителем рубежа охраны путем использования ухищренных способов передвижения необходимо устанавливать несколько СО, как правило, различных физических принципов действия, рассчитанных на блокирование участка при разных способах передвижения нарушителя. Для открытых пространств скорость движения может изменяться от 0,1 до 8 м/с, способы перемещения - от движения "ползком" до движения "в рост"; для физических преград (например, двери и ставни) способами преодоления могут быть открывание и разрушение (полное или частичное). Аналогично рассматриваются способы преодоления замкнутых пространств, а также стен, перекрытий и т.п.

Для предотвращения возможности имитации работы СО нарушителем соединительные линии системы сбора, обработки, отображения и документирования информации (ССОИ) должны иметь физическую и сигнализационную защиту коммутационных шкафов, коробок и т.п. При прокладке кабелей предпочтение следует отдавать скрытой проводке в закладных устройствах (трубах), обеспечивающих дополнительное экранирование и инженерную защиту.

В настоящее время выпускается большое число ССОИ, различающихся числом подключаемых СО, структурой соединительных линий - радиальная (лучевая), шлейфовал (магистральная), древовидная, петлевая (кольцевая) и другими характеристиками. Это позволяет оборудовать объект любого размера наперед заданной группы важности и/или категории защиты. Учет возможности вывода из строя ТСОС подготовленным и технически оснащенным нарушителем проводится при анализе возможных структурных схем построения ТСОС и КТСО в целом. При этом из рассмотрения должны быть исключены варианты, позволяющие замыканием (коротким замыканием) шин питания или информационно-адресных шин КТСО вывести его из строя. Для современных КТСО характерно использование лучевой или древовидной структуры информационно-адресных шин, раздельного управления и автономных защитных цепей электропитания каждого канала.

Ниже рассмотрим некоторые основные требования к выбору аппаратуры ССОИ, определяемые возможностью появления подготовленного и технически оснащенного нарушителя и степенью его подготовки и оснащенности. Возможность обхода ССОИ подготовленным и технически оснащенным нарушителем учитывается при выборе способа передачи информации в ССОИ. Различают три типа аппаратно-программной реализации ССОИ:

1. тип - с низкой устойчивостью к обходу;
2. тип - со средней устойчивостью к обходу;
3. тип - с высокой устойчивостью к обходу.

Под низкой устойчивостью ССОИ к обходу понимают такую организацию опроса СО в АСО, при которой при снятии участка (СО) с охраны состояние соединительной линии и датчика вскрытия СО со стороны АСО не контролируются (отсутствует режим "деблокирование").
Под средней устойчивостью понимают такую организацию опроса СО в АСО, при которой при снятии участка (СО) с охраны состояние соединительной линии и датчика вскрытия СО остаются под контролем АСО (имеется режим "деблокирование").
Под высокой устойчивостью понимают организацию опроса СО, аналогичную средней, но сообщения шифруются с использованием кода, гарантированная стойкость которого к обходу (дешифрации) составляет десятки тысяч часов.
Для предотвращения преодоления ТСО путем оказания воздействия на оператора системы охраны или использования его негативных качеств ССОИ должна иметь режим документирования и иерархическую систему управления, т.е. оператор не должен иметь полного контроля над ССОИ, необходимого лишь при ее настройке, а в системе охраны больших объектов оператор не должен обладать и возможностью снятия (постановки) некоторых участков охраны.
Для того чтобы оперативно обнаружить выход из строя составных частей КТСО, в том числе и в случае преднамеренных действий (саботажа), применяется дистанционный контроль (автоматизированный или автоматический), обеспечивающий проверку работоспособности СО, соединительной линии и приемной аппаратуры ССОИ, а также повышающий устойчивость ТСОС к обходу соединительных линий и имитации работы СО.

2. Системный подход-основа методологии разработки концепции комплексного обеспечения безопасности объектов охраны

Как показали результаты многих исследований, для выработки системного решения, удовлетворяющего необходимым и достаточным условиям обеспечения надежной защиты ОО от подготовленного и технически оснащенного нарушителя, требуется полный учет не только перечисленных выше факторов, но и многих других, как то: состояние инженерных сооружений объекта, состав и уровень подготовки сил физической охраны объекта, окружение объекта, характер объекта (легендируемый, нелегендируемый), расположение и количество сил поддержки, состояние сетей электропитания объекта и т.д.
Многолетний опыт по созданию систем защиты объектов убеждает в безусловной необходимости разрабатывать в каждом случае **системную концепцию обеспечения безопасности** конкретного объекта, которая на практике предполагает комплексное взаимоувязанное решение руководством предприятия и службой безопасности (охраны) ряда крупных блоков задач (часть из которых могут решаться лишь с помощью спецслужб при строгом соблюдении соответствующих законов РФ), как то:

1. **Определение стратегии комплексной безопасности.** Здесь решаются проблемы классификации, систематизации и дифференциации угроз; определяются структура и задачи служб безопасности; разрабатываются (определяются) нормативно-правовые документы, регламентирующие с позиций юриспруденции деятельность служб безопасности (СБ); на основе анализа ресурсов, технико-экономических показателей и социальных аспектов безопасности разрабатываются планы мероприятий по обеспечению безопасности объектов.
2. **Обеспечение безопасности от физического проникновения на территорию и в помещения объекта.** В этом блоке задач на основе анализа доступности объекта моделируются стратегия и тактика поведения потенциального нарушителя (по всем возможным моделям нарушителей); дифференцируются зоны безопасности; на основе определения ключевых жизненно важных центров объектов разрабатываются принципы и схемы оборудования техническими средствами охранной сигнализации и телевизионного наблюдения, средствами инженерной, технической и специальной защиты рубежей

охраны (периметра, территории, зданий, помещений, хранилищ, сейфов, транспортных коммуникаций, средств связи, компьютерных сетей и т.д.). Соответственно, на основе расчета тактико- технических требований выбирается состав и номенклатура технических средств.

3. **Защита информации.** Решение задач данного блока обеспечивается специальными методами защиты. На основе разработки принципов проверки, классификации источников информации и каналов ее утечки разрабатываются концептуальные модели защиты от утечки информации, проводятся их оценки на предмет эффективности предлагаемых этими моделями решений. Здесь решается широкая гамма задач разработки методов защиты по всем возможным каналам утечки (речевой, визуальный, виброакустический, электромагнитный, проводной, за счет паразитных связей и наводок и др.). Разрабатывается нормативная база по защите от утечки информации. На основе моделирования возможных способов приема информации потенциальным нарушителем за пределами помещений посредством применения направленных микрофонов, лазерных средств и т.п. вырабатываются методы пассивной и активной защиты.

4. **Защита от прогнозируемых к применению средств внегласного контроля.** Эти задачи ориентированы на модель нарушителя - сотрудника учреждения, либо на проведение контрразведывательных мероприятий, если по оперативным каналам получена информация о заинтересованности, которую проявили организованные преступные формирования к данному объекту. Здесь решается ряд специфических задач от выбора и установки средств негласного контроля до выбора организационно-режимных мер защиты от негласного контроля со стороны потенциального нарушителя. Большое внимание здесь уделяется техническим средствам дефектоскопии, автоматизации средств контроля трактов передачи информации, анализу системы демаскирующих признаков и ряду других [*].

5. **Защита от диверсионно-террористических средств (ДТС).** Задачи данной предметной области также решаются специальными методами защиты. На основе исследования, классификации и моделирования вариантов активных действий террористов, прогнозирования возможных способов доставки ДТС на территорию объекта, изучения каналов управления диверсиями и технических способов их осуществления (например, с использованием радиовзрывателей) выбирается аппаратура обнаружения ДТС, разрабатываются организационно-технические мероприятия по созданию контрольных пунктов, постов проверки, использованию меточной техники и ряд других. Разрабатываются рекомендации по выбору техники обнаружения.

6. **Обеспечение безопасности (защита информации) в локальных вычислительных сетях (ЛВС) и ПЭВМ, т.е. в автоматизированных системах обработки информации (АСОИ).** Здесь на основе анализа моделей нарушителей, классификации видов угроз и видов компрометации информации разрабатывается комплексный подход к защите информации в автоматизированных информационных системах, ЛВС, серверах и ПЭВМ, соответствующая нормативно- правовая база защиты, регламентирующие документы; разрабатываются методы и способы программно-аппаратной защиты от несанкционированного доступа и копирования (НСД, ИСК). Особое место занимают разработка и внедрение специальных математических и программных методов защиты операционных систем, баз данных и серверов, методов идентификации пользователей и ЭВМ, паролей, ключей и антивирусных программ. На основе определения и анализа задач СБ разрабатываются организационные меры защиты.

Этот блок задач достаточно подробно рассмотрен в книге [100].

7. **Защита систем связи.** С точки зрения проведения разведывательных операций со стороны ОПФ (Г) необходимость тщательной разработки данного блока задач является чрезвычайно актуальной, ибо наиболее доступными для перехвата нарушителем информации, безусловно, являются каналы связи.

Здесь на основе классификации сетей связи разрабатываются методы оптимизации связи, криптографической защиты, защиты телефонных сетей связи. Наряду с решением проблем стандартизации защиты, создаются специальные методы и способы, обеспечивающие конфиденциальную связь.

8. Человеческий фактор в системе обеспечения безопасности. Здесь рассматривается блок задач, решаемый детективной группой службы безопасности, как то:

- разработка и реализация мероприятий по изучению лиц из числа персонала и иных лиц, в действиях которых содержатся угрозы безопасности деятельности учреждения посредством воздействия на его сотрудников, их близких и родственников;
- проверка кандидатов для приема на работу;
- разработка и реализация мероприятий по обеспечению "чистоты рук";
- организация взаимодействия и поддержание контактов с силами поддержки и/или правоохранительными органами по вопросам обеспечения безопасности и многое другое.

9. Исследование средств отечественного и зарубежного вооружения, которые могут применяться для поражения объектов. В данном блоке задач должны быть рассмотрены возможные способы и применяемые организованными преступными формированиями (или исполнителями - одиночками) виды вооружения, взрывчатых или иных поражающих веществ для осуществления вооруженной акции.

Здесь на основе анализа тактико-технических характеристик традиционных и нетрадиционных средств поражения объектов должна быть дана классификация этих средств, описаны характерные признаки их поражающего действия, методы и способы их обнаружения, локализации, обезвреживания или уничтожения, а также проведена оценка эффективности систем охраны и обороны объектов.

10. Организация системы контроля доступа. Этот блок задач направлен на эффективную реализацию процедур проверки человека, пытающегося открыто ("законным образом") проникнуть на территорию объекта, в отдельные его помещения и режимные зоны. Здесь решаются задачи идентификации - это установление тождества (опознание личности) по совокупности общих и частных признаков и аутентификации - это установление подлинности личности (см. например [5, 55, 168]).

Кроме 10 перечисленных (которые напрямую связаны с оперативной охранной деятельностью) существуют иные блоки задач, рассматривающих как общесистемные проблемы, например, определение приоритетов (иерархий) во взаимодействии элементов системы безопасности, так и специальные, например обеспечение пожарной безопасности. Области охранной деятельности, связанные с реализацией названных задач, чрезвычайно многогранны. В данной книге рассматриваются лишь основы теории создания технических средств охраны, с помощью которых обеспечивается защита объекта охраны от физического проникновения нарушителя, т.е. решение второго блока задач (в американской литературе в данном случае применяется понятие "система физической защиты", см., например, М. Гарсия. Проектирование и оценка систем физической защиты / Пер. с англ.; Под ред. Р.Г. Магауенова. - М.: "Мир", 2002.).

Взаимоувязанное решение перечисленных блоков задач **системной концепции обеспечения безопасности объекта,** в каждом из которых существуют свои подходы, методы и способы решения, должно обеспечить непротиворечивость и полноту принимаемых мер защиты. Только в этом случае можно говорить о выполнении **необходимых и достаточных условий** в деле защиты объекта от подготовленных и технически оснащенных нарушителей.

Реализация каждого из блоков задач осуществляется посредством разработки проекта, который носит индивидуальный для учреждения и объекта (территории, здания, этажа, помещения) характер. В зависимости от категории важности объекта этот проект должен обладать соответствующими грифами секретности. Однако и для нережимных объектов охраны такой проект должен носить строго конфиденциальный характер, т.е. быть

доступным строго ограниченному кругу лиц из числа сотрудников СБ(0) и руководства.
Необходимость комплексного решения (на основе системного подхода) перечисленных основных (типовых) блоков задач проистекает из того, что профессионализму ОПФ (Г), безусловно, следует противопоставить организацию и оснащение, выполненные на более высоком уровне профессионализма. Однако, коль скоро абсолютной защищенности быть не может, в каждом случае проводятся сравнительные оценки затрат на защиту и возможные потери при сознательном отказе от применения несоизмеримо дорогостоящих (относительно потерь) методов и технических средств защиты.
В мировой практике уже давно используется такое понятие как система защиты, под которой подразумевается комплекс организационных и технических мероприятий, направленных на выявление и противодействие различным видам угроз деятельности объекта.
Рассмотрение возможных угроз проводится по следующим основным направлениям:

- безопасность персонала: неэффективная защита может привести к ущербу здоровью или даже угрозе жизни сотрудников;
- угрозы материальным ценностям, имуществу и оборудованию;
- безопасность информации.

Существенным при оценке угроз и выборе приоритетов в системе защиты является учет международного опыта по организации охранной деятельности применительно к объектам конкретного вида, например, банков, предприятий, крупных офисов и т.д. Этот опыт берется за основу и при подготовке современных нормативов защиты. Так, например, западно-европейские фирмы

- производители оборудования для систем банковской защиты придерживаются единых критериев оценки угроз, согласно которым для сейфовых комнат - хранилищ ценностей и компьютерной информации приоритеты направлений защиты следующие (более подробно см. Концепция комплексной защиты банковских объектов. - М.: Росси Секьюрити, 1998.):
- терроризм, стихийные бедствия и аварии, пожары, наводнения, механическое разрушение;
- несанкционированный (неразрешенный) съем информации из компьютерного банка данных;
- несанкционированное проникновение в сейфовую комнату как с целью кражи ценностей, так и с целью кражи информации.

Несмотря на существенные различия в природе угроз, создание защиты от каждой из них должно идти в комплексе со всей системой. Например, несанкционированный съем информации может осуществляться дистанционно путем контроля из соседнего здания излучений от средств обработки банка данных, в котором может содержаться информация конфиденциального характера. Защитой от такого вида угрозы является экранирование аппаратуры и коммуникаций, применение специальной аппаратуры, искажающей картину электромагнитного поля излучения. Но съем информации можно проводить и с помощью специально внедренных в помещение подслушивающих устройств, как то: микрофоны, радиозакладки и т.п. (см. примечание на с. 22). Защитой в этом случае будет поиск техники подслушивания с привлечением компетентных органов, а также строгое соблюдение режима доступа в помещение или в здание, что является защитой и от несанкционированного проникновения.
В основе разработки системы защиты объекта и организации ее функционирования лежит принцип создания последовательных рубежей, в которых угрозы должны быть своевременно обнаружены, а их распространению будут препятствовать надежные преграды. Такие рубежи (зоны безопасности) должны располагаться последовательно от ограждения вокруг территории объекта до главного особо важного помещения, такого как хранилище материальных и информационных ценностей.

Защита объекта должна состоять из различного рода ограждений его периметра и специально оборудованных въездов и проходов, решеток на окнах и в дверных проемах, резервных выходов из здания, охранной сигнализации, охранного освещения и охранного теленаблюдения.

Элементы защиты всех участков объекта должны взаимодополнять друг друга. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по максимуму времени, которое злоумышленник затратит на преодоление всех зон безопасности. За это же время должна сработать сигнализация, сотрудники охраны установят причину тревоги, примут меры к задержанию злоумышленника и вызовут подкрепление из ближайшего отделения милиции или из сил поддержки.

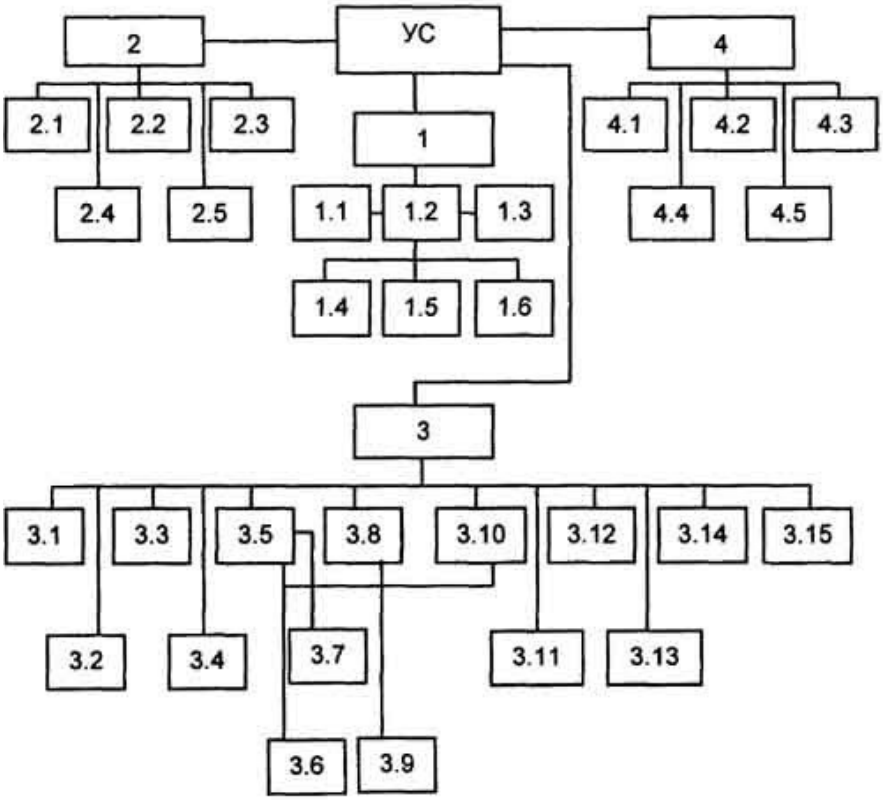


Рис. 3. Укрупненная структурная схема системы обеспечения безопасности объекта

Таким образом, эффективность системы защиты оценивается величиной времени с момента возникновения угрозы до начала противодействия или ликвидации ее. Чем более сложная и разветвленная система защиты, тем больше времени потребуется на ее преодоление и тем больше вероятность того, что угроза будет своевременно обнаружена, определена и отражена.

Современные системы безопасности основываются на реализации комплекса мероприятий по организации физической, инженерной, технической и специальной защиты.

В общем виде укрупненная структурная схема системы обеспечения безопасности объекта представлена на рис. 3. На рис. 3 приняты следующие обозначения:

УС - укрупненная структурная схема системы обеспечения безопасности объекта

- 1 - физическая защита
- 1.1 - объектовая и/или городская пожарная команда
- 1.2 - служба охраны
- 1.3 - наряд милиции и/или силы поддержки
- 1.4 - работники контрольно-пропускного поста
- 1.5 - операторы технических средств охраны
- 1.6 - тревожная группа и подвижные посты

- 2 - инженерная защита
- 2.1 - усиленные ограждающие конструкции
- 2.2 - усиленные двери и дверные коробки
- 2.3 - металлические решетки и жалюзи
- 2.4 - спецзамки, усиленные запоры
- 2.5 - сейфы повышенной стойкости
- 3 - техническая защита
- 3.1 - средства обнаружения радиоактивных средств
- 3.2 - средства обнаружения оружия
- 3.3 - система пожарной сигнализации
- 3.4 - система тревожного оповещения
- 3.5 - система контроля доступа
- 3.6 - охранное освещение
- 3.7 - переговорные устройства
- 3.8 - система охранной сигнализации
- 3.9 - источник резервного электропитания
- 3.10 - система телевизионного наблюдения
- 3.11 - средства связи
- 3.12 - средства проверки почтовой корреспонденции
- 3.13 - средства обнаружения взрывчатых веществ
- 3.14 - система защиты средств ВТ и ЛВС
- 3.15 - средства обнаружения и защиты от технических средств проникновения через инженерные коммуникации, отверстия, проёмы и т.д.
- 4 - специальная защита (см. примечание на с. 22)
- 4.1 - обеспечение требований безопасности на этапе строительства
- 4.2 - проведение обследования помещений на наличие устройств съема информации
- 4.3 – спецпроверка технических средств передачи, обработки, накопления и хранения информации
- 4.4 - специальные защищенные помещения для переговоров
- 4.5 - средства спецзащиты сетей коммуникации

Физическая защита обеспечивается службой охраны, основной задачей которой является предупреждение несанкционированного физического проникновения на территорию, в здания и помещения объекта злоумышленников и их сдерживание в течение расчетного времени (до прибытия милиции или сил поддержки).

Инженерная защита предусматривает использование усиленных дверей и дверных коробок, металлических решеток, усиленных ограждающих конструкций, усиленных запоров, сейфов повышенной стойкости.

Техническая защита включает систему охранной сигнализации, систему телевизионного наблюдения, систему тревожного оповещения, автоматизированную систему контроля доступа, переговорные устройства, средства связи, пожарной сигнализации, средства проверки почтовой корреспонденции, охранного освещения, резервного (аварийного) электропитания, систему дежурного и тревожного освещения.

Не лишним может оказаться и установка детекторов оружия (металлоискателей) и средств контроля радиационной обстановки на входе здания для предотвращения возможности проведения терактов.

Специальная защита обеспечивает защиту от утечки информации, представляющей особую ценность, а также проверку надежности (лояльности) персонала службы охраны, материально ответственных лиц и некоторых других категорий служащих.

Специальная защита состоит из комплекса организационно-технических и специальных мероприятий, предусматривающих:

- обеспечение требований безопасности на этапах проектирования, строительства

(реконструкции) и эксплуатации зданий;

- периодическое проведение специальных обследований отдельных помещений для выявления возможно установленных в них подслушивающих устройств;
- сооружение специальных технически защищенных помещений для ведения конфиденциальных переговоров и контроль работоспособности специальных средств защиты;
- проверку и защиту технических средств, используемых для передачи, обработки, накопления и хранения конфиденциальной информации;
- оборудование средствами защиты электросети, внутренней и городской телефонной связи и других коммуникаций систем жизнеобеспечения;
- осуществление специальных проверочных мероприятий по выявлению неблагонадежных сотрудников и лиц с психическими отклонениями (автоматизированные системы психологического тестирования).

Как показывает опыт зарубежных фирм и отечественных организаций и предприятий, нормальное, безущербное функционирование возможно лишь при системном, взаимоувязанном использовании всех вышеназванных видов защиты и четко спланированных действиях сил службы охраны по сигнальной информации, получаемой от средств системы технической защиты.

Таким образом, мы вкратце рассмотрели основные положения обобщенной системной концепции обеспечения безопасности ОО.

3. Общий подход к категорированию объектов охраны

Основополагающими, определяющими выбор уровня защиты объекта, признаками являются категория важности объекта и модель нарушителя, от проникновения которого данный объект должен быть защищен.

Система охраны объекта, т.е. его периметра, территории, зданий, помещений - это сложный, многорубежный комплекс, включающий в себя физическую защиту (личный состав охраны), инженерные сооружения (решетки, стальные двери, сложные замки, замки - защелки, сейфы и т.п.), технические средства охранной сигнализации, системы телевизионного наблюдения (СТН), системы контроля доступа (турникеты, шлагбаумы, управляемые ворота и т.д.) и многое другое, что было рассмотрено в структурной схеме системы обеспечения безопасности объекта (см. рис. 3).

Создание технически высокооснащенной системы охраны чрезвычайно дорогостоящее дело, поэтому разработчики КТСО и СБ (О) (исполнители и заказчики) выбирают такую конфигурацию и архитектуру КТСО, которая была бы экономически разумной. Это означает, что затраты на создание, внедрение и эксплуатацию КТСО должны быть существенно ниже, чем стоимость того, что охраняется. По некоторым оценкам эти затраты составляют около 5% основных фондов и до 25% оборотных средств в расчете на один финансовый год.

Существуют определенные методики технико-экономических обоснований выбора того или иного варианта оборудования объекта ТСОС, например [187]. Однако очевидно, что для объектов особого риска, как например, ядерноопасных объектов, на которых проведение диверсионно- террористических актов может повлечь за собой неисчислимые бедствия, гибель людей, разрушение экологической системы целых регионов, требуются достаточные для их надежной защиты затраты.

Таким образом, абстрактно-типизированный подход к категорированию важности объектов (далее для краткости - категорированию объектов) необходим лишь для приближенной оценки возможных затрат на их оснащение инженерно-техническими, специальными и аппаратно- программными средствами защиты.

Второй аспект, влияющий на уровень затрат, т.е. в конце концов на выбор уровней защиты - это модель нарушителя. Например, очевидно, чем выше должностной статус злоумышленника, работающего на охраняемом объекте (например, им может быть

"директор", "главный инженер" и т.д.), тем выше будут затраты на создание системы безопасности, адекватной их "моделям". Поэтому следует понимать, что абсолютной защищенности объекта быть не может. Но это уже проблемы, выходящие далеко за рамки категорирования объектов, создания и применения КТСО, хотя и в определенной мере связанные с ними.

Итак, в данном изложении определение необходимых уровней защиты мы будем связывать с понятием классификации объектов по категориям важности, полагая априори, что злоумышленник является человеком "со стороны".

В первом приближении при выборе уровня защиты следует учитывать возможность обоснованного отнесения объекта к одной из четырех категорий:

- 1-я категория - особо важный объект;
- 2-я категория - особо режимный объект;
- 3-я категория - режимный объект;
- 4-я категория - нережимный объект.

Отнесение конкретных объектов к той или иной категории важности регламентируется специальным перечнем, утвержденным правительством РФ.

В относительно самостоятельных (национальных, областных, краевых) территориальных образованиях могут создаваться свои перечни объектов, дополняющие общий, исходя из требований местных условий и возможностей самостоятельного финансирования расходов по их оснащению КТСО.

Очевидно, что выбор уровня оснащения КТСО названных категорий объектов будет зависеть от многих конкретных факторов, как то: конфигурация территории, рельеф местности, географическое положение, структура расположения жизненно важных центров объекта, характер угроз и т.д.

Априори следует полагать:

- *1-я и 2-я категории объектов* требуют высокого уровня оснащения КТСО, включения в него разнообразных ТСОС, телевизионных средств наблюдения (ТСН), наличия развитой ССОИ, СКД, создания многих рубежей защиты (зон безопасности), реализации функций автоматического определения направления движения нарушителя, состояния СО, анализа характера разрушающего действия нарушителя на КТСО и т.д.;
- *3-я категория объектов* требует меньшего, но достаточно высокого уровня оснащения. Здесь выборочно исключается исполнение ряда функций охраны (защиты), затраты на реализацию которых заведомо выше возможных потерь от злоумышленных действий;
- *4-я категория объектов* оснащается КТСО ограниченной структуры, предполагает наличие меньшего числа зон безопасности, реализацию меньшего количества функций в ССОИ.

Следует отметить, что наряду с категорированием объектов должно применяться и категорирование помещений с организацией соответствующих "зон безопасности". Это позволит минимизировать затраты на оснащение КТСО и организацию системы защиты в целом. Выбор категории (уровня защиты) должен осуществляться исходя из значимости объекта, характера потенциальных угроз и, соответственно, "моделей" вероятных нарушителей и моделей их вероятных действий.

Приведенная классификация категорий важности объектов представляет по существу лишь укрупненно-базисный подход. В специальных разработках по этой проблеме выделяются множества подклассов, на основе чего разрабатываются идеи типизации объектов и решения соответствующих задач типизации их оснащения КТСО.

Наиболее опасной угрозой для любого объекта является угроза проведения диверсионно-террористического акта (ДТА) с применением диверсионно- террористических средств (ДТС).

Коль скоро невозможно ставить задачу защиты всех без исключения или абсолютного большинства объектов, ибо это непосильно из-за невероятно больших затрат финансовых,

материальных и людских ресурсов, принят подход, в рамках которого решаются задачи определения перечня типовых особо важных объектов народного хозяйства, МО и иных (требующих охраны) объектов. Этому подходу характерна разработка рациональных (типовых) схем защиты объектов, входящих в группу риска, исходя из вероятности использования на них ДТС или их привлекательности для преступных посягательств.

Исходя из международного опыта следует, что противодействие преступности, особенно ОПФ, может осуществляться лишь на основе государственной программы борьбы с преступностью. При этом приоритетный выбор объектов для организации системной защиты определяется, исходя из оценки возможного использования на них ДТС.

Типовые особо важные объекты, как правило, принадлежат таким отраслям как энергетика, транспорт, химические и нефтехимические, наука и техника, оборонная промышленность, оборона, связь и информатизация, а также Министерствам финансов, здравоохранения, культуры и силовым структурам страны. Эти отрасли являются ключевыми для жизнеобеспечения общества и от их действенной защиты зависит жизнь, спокойствие и морально- психологическое состояние всего народа, прогрессивность движения общества, результативность экономических преобразований.

Лабораторное занятие №9.
Тема: Аналитический подход к классификации угроз безопасности информационного объекта на основе моделирования нарушителей и их действи

СОДЕРЖАНИЕ ЗАНЯТИЯ

"Модель" нарушителя, возможные пути и способы его проникновения на охраняемый объект. Вопросы классификации нарушителей и угроз информационной безопасности
Характеристика нарушителя, степень его подготовки и оснащенности, общие рекомендации по применению технических способов защиты. В начале данной главы достаточно подробно говорилось о том, что охрана объекта является сложным интегрированным процессом. В широком смысле под охраной понимается комплекс организационных, контрольных, инженерно-технических и иных мероприятий, направленных на обеспечение полной, частичной или выборочной защиты информации, материальных ценностей и безопасности персонала объекта.
В узком смысле задача системы охраны заключается в обнаружении и пресечении действий людей, пытающихся тайно или открыто (но несанкционированно) проникнуть на охраняемую территорию объекта или в его зоны безопасности.
Как показывает опыт работы, нормальное безущербное функционирование системы защиты возможно при комплексном использовании всех видов защиты (изложенных в системной концепции) и четко спланированных действиях сил службы охраны по сигналам, получаемым от технических средств охранной сигнализации.
Охрана учреждения, как правило, является достаточно дорогостоящим мероприятием, поэтому при выборе уровня защиты целесообразно оценить возможные потери от "беспрепятственного" действия нарушителя и сравнить их с затратами на организацию охраны. Этот показатель является индивидуальным для каждого объекта и может быть оценен, как правило, весьма приближенно. Практика создания и эксплуатации комплексов технических средств охранной сигнализации показала, что в большинстве случаев для построения эффективной охраны требуется наличие комбинированных ТСОС, учитывающих возможность дублирования функций обнаружения на основе использования различных физических принципов действия средств обнаружения (близкие понятия - синонимы: датчиков, детекторов, извещателей).
В основе эффективного противодействия угрозе проникновения нарушителя в охраняемые помещения (сейфовые комнаты, переговорные помещения, архивы конструкторско-технологической документации, хранилища информационных баз данных и т.п.) лежит проведение априорных оценок:

- - приоритетов в системе защиты (т.е. следует определить, что может представлять наибольший интерес для нарушителя и должно защищаться в первую очередь);
- - путей возможного проникновения нарушителей;
- - информации, которой может располагать нарушитель об организации системы защиты предприятия;
- - технических возможностей нарушителя (его технической вооруженности) и т.д., т.е. оценок совокупности количественных и качественных характеристик вероятного нарушителя.

Такая совокупность полученных оценок называется "моделью" нарушителя. Эта модель, наряду с категорией объекта, служит основой для выбора методов организации охраны объекта, определяет сложность и скрытность применяемых технических средств охранной сигнализации и телевизионного наблюдения, варианты инженерно-технической защиты, кадровый состав службы охраны и т.д.
По уровню подготовки и технической оснащенности "нарушителя" условно можно разделить на следующие типы:

- - случайные (не знающие, что объект охраняется и не имеющие специальной цели

проникновения на объект);

- - неподготовленные (проникающие на объект со специальной целью и предполагающие возможность охраны объекта, но не имеющие информации о структуре и принципах действия системы охраны);
- - подготовленные (имеющие информацию о возможных методах обхода ТСО и прошедшие соответствующую подготовку);
- - обладающие специальной подготовкой и оснащенные специальными средствами обхода;
- - сотрудники предприятия (последние два типа нарушителей можно объединить термином "квалифицированный").

Наиболее распространенной "моделью" нарушителя является "неподготовленный нарушитель", т.е. человек, пытающийся проникнуть на охраняемый объект, надеясь на удачу, свою осторожность, опыт или случайно ставший обладателем конфиденциальной информации об особенностях охраны. "Неподготовленный нарушитель" не располагает специальными инструментами для проникновения в закрытые помещения и тем более техническими средствами для обхода охранной сигнализации. Для защиты от "неподготовленного нарушителя" часто оказывается достаточным оборудование объекта простейшими средствами охранной сигнализации (лучевые средства обнаружения на периметре, кнопки или магнитоуправляемые контакты на дверях в помещения) и организация службы невооруженной охраны (имеющей пульт охранной сигнализации и телефонную связь с милицией).

Более сложная "модель" нарушителя предполагает осуществление им целенаправленных действий, например, проникновение в охраняемые помещения с целью захвата материальных ценностей или получения информации. Для крупного учреждения наиболее вероятной "моделью" является хорошо подготовленный нарушитель, возможно действующий в сговоре с сотрудником или охранником. При этом возможны такие варианты проникновения, как:

- - негласное проникновение одиночного постороннего нарушителя с целью кражи ценностей, для установки специальной аппаратуры или для съема информации;
- - негласное проникновение нарушителя-сотрудника предприятия с целью доступа к закрытой информации;
- - проникновение группы нарушителей в охраняемые помещения в нерабочее время путем разрушения инженерной защиты объекта и обхода средств охранной сигнализации;
- - проникновение одного или группы вооруженных нарушителей под видом посетителей (в рабочее время, когда не введены в действие все средства инженерной и технической защиты) с целью силового захвата ценностей;
- - вооруженное нападение на объект с целью захвата заложников, ценностей, получения важной информации или организации собственного управления.

Очевидно, "модель" нарушителя может предполагать и сразу несколько вариантов исполнения целей проникновения на ОО.

Среди путей негласного проникновения нарушителя прежде всего могут быть естественные проемы в помещениях: двери, окна, канализационные коммуникации, кроме того непрочные, легко поддающиеся разрушению стены, полы, потолки. Поэтому при организации охранной сигнализации в охраняемом помещении в первую очередь должны быть установлены средства обнаружения для защиты окон и дверей. Обнаружение проникновения через стены, полы и потолки выполняют, как правило, СО, предназначенные для защиты объема помещения. Для усиления защиты окон и дверей широко используются металлические решетки и защитные жалюзи. Установка достаточно надежных решеток на окна может иногда позволить отказаться от установки на них средств охранной сигнализации. Однако часто наблюдалось, что неправильная конструкция решеток открывает дополнительные возможности для проникновения в здание. Например, защищая окна первого этажа, решетки могут облегчить доступ к окнам

второго этажа.
Возможность проникновения на объект вооруженных нарушителей требует не только усиления вооруженной охраны, но и установки на входах обнаружителей оружия, оборудование особо ответственных (важных) рабочих мест сотрудников кнопками и педалями тревожного оповещения, а в ряде случаев и установки скрытых телекамер для наблюдения за работой сотрудников. Входы в хранилища ценностей должны оборудоваться специальными сейфовыми дверями с дистанционно управляемыми замками и переговорными устройствами.
Уровни технической оснащенности нарушителя и его знаний о физических принципах работы СО, установленных на объекте, определяют возможность и время, необходимое ему на преодоление средств инженерной защиты и обход сигнализационной техники. Наиболее эффективны СО, физический принцип действия и способ обхода которых нарушитель не знает. В этом случае вероятность его обнаружения приближается к единице (что определяется только техническими параметрами самого СО).
В конечном счете, поскольку задачей системы охраны является оказание противодействий нарушителю в достижении его целей, при построении системы охраны в ее структуру закладывается принцип создания последовательных рубежей на пути движения нарушителя. Угроза проникновения обнаруживается на каждом рубеже и ее распространению создается соответствующая преграда. Такие рубежи (зоны безопасности) располагаются последовательно от прилегающей к зданию территории до охраняемого помещения, сейфа. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по минимальному значению времени, которое нарушитель затратит на преодоление всех зон безопасности. За это время, с вероятностью близкой к 1, должна сработать система охранной сигнализации. Сотрудники охраны установят причину тревоги (например, с помощью телевизионной системы наблюдения или путем выдвижения на место тревожной группы) и примут необходимые меры.
Если "модель" нарушителя рассматривает негласное проникновение в охраняемое помещение нарушителя-сотрудника (в том числе из службы охраны), в состав средств охранной сигнализации необходимо включить устройства документирования работы средств обнаружения, чтобы фиксировать несанкционированные отключения каналов сигнализации. Обычно указывается время постановки и снятия с охраны помещения. Аппаратура документирования должна устанавливаться в специальном помещении, куда имеют доступ только начальник охраны или ответственный сотрудник службы безопасности.
Итак, сложность системы охраны, ее насыщенность средствами инженерной и технической защиты определяются "моделью" нарушителя, категорией и особенностями объекта охраны. Количество необходимых зон безопасности определяется, исходя из состава материальных и информационных ценностей, а также специфических особенностей самого объекта. Если объект расположен в здании с прилегающей к нему территорией, то ограждение и периметральная охранная сигнализация образуют первую зону безопасности объекта. Последней зоной безопасности, например сейфовой комнаты, будет специальный сейф с кодовым запирающим устройством и сигнализационным средством, передающим информацию о попытках его вскрытия.
Очевидно, что для разработки "модели" нарушителя применительно к некоторому ОО необходимо обобщение большого опыта как отечественной, так и зарубежной практики построения систем охраны объектов, аналогичных рассматриваемому. С течением времени "модель" нарушителя, а следовательно, и вся концепция
охраны могут меняться. Отсюда следует вывод о необходимости периодического дополнения концепции охраны объекта, обновления системы инженерной защиты, системы охранной сигнализации, телевизионного наблюдения, системы контроля доступа и всех иных систем, рассматриваемых системной концепцией обеспечения безопасности.

Способы получения "нарушителем" информации об объекте и технических способах защиты объекта, вероятные пути проникновения. Целями "нарушителя" или "нарушителей", проникающих на объект, как отмечалось выше, могут быть: кража материальных и/или информационных ценностей, установка закладных устройств, разрушение объекта, захват заложников, а возможно и захват управления функционированием объекта. Злоумышленник будет искать наиболее оптимальные (менее опасные для себя) пути проникновения в нужное ему помещение для осуществления поставленной противозаконной (преступной) цели, будет стараться оставить как можно меньше следов своих действий, разрушений. С этой целью он будет изучать обстановку на объекте, алгоритм охраны, неохраняемые переходы, помещения, способы и условия хранения ценностей.

Применение систем охранной сигнализации с высокими тактико-техническими характеристиками на всех возможных путях движения "нарушителя" совместно с инженерной и физической защитой позволит достаточно надежно защитить объект на требуемом (заданном априори) уровне.

Таким образом, неоспорима важность принятия мер, максимально затрудняющих получение "нарушителем" сведений об основных характеристиках технических средств охраны, их принципе действия, режимах работы.

В то же время некамуфлируемость средств охранной сигнализации в местах скопления посетителей, распространение слухов об их сложности, уникальности и невозможности их "обойти" будет способствовать отпугиванию некоторых потенциальных "нарушителей".

Наиболее вероятными путями физического проникновения "нарушителя" в здание являются:

- через двери и окна первого этажа;
- по коммуникационным и техническим проемам подвала или цокольного этажа;
- с крыши через окна или другие проемы верхних этажей;
- путем разрушения ограждений (разбивание стекол, пролом дверей, решеток, стен, крыши, внутренних перегородок, пола и т.п.);
- имеются и иные способы, связанные с применением нарушителем специальных технических средств (все эти сведения легко почерпнуть из телефильмов, телепередач на криминальные темы, детективов и т.д.).

Необходимо максимально предусмотреть физические преграды перед нарушителем на пути его движения к материальным и информационным ценностям.

Внутренние переходы, подходы к наиболее важным помещениям должны быть оснащены не только средствами охранной сигнализации и телевизионного наблюдения, но и иметь надежную инженерную защиту в виде тамбуров с дистанционно управляемыми дверями, решетками, а сами хранилища ценностей - укрепленными перегородками.

Готовясь к преступлению, "нарушитель", используя легальную возможность посетить учреждение, ходит по некоторым его помещениям, может тщательно изучить наименее охраняемые места, расположение постов охраны, действия охранников при проходе сотрудников в различные режимные зоны. В этом случае очень важно разделять потоки клиентов учреждения от сотрудников. Проходы, помещения, где клиенты не обслуживаются, должны иметь кодовые замки или средства контроля доступа.

Некоторые подробности режима охраны преступник может получить, "разговорив" кого-либо из сотрудников учреждения или охраны.

Наибольшую опасность представляют сотрудники охраны, вступившие в преступную связь с "нарушителем". От них можно получить информацию и о принципах работы аппаратуры охранной сигнализации, ее режимах, "слабых" местах, оптимальных путях проникновения в требуемые помещения, а в решающий момент они могут отключить отдельные каналы охранной сигнализации. В связи с этим станционная аппаратура охранной сигнализации должна иметь систему документирования, должны протоколироваться дата и время включения/выключения каналов сигнализации, режимы

проверки неисправности аппаратуры с фиксацией даты и времени происшедшего сбоя, отключения на профилактику и т.д.

Информация о состоянии охраны на объекте, оптимальных путях движения к требуемому помещению и путях отхода нужна любому "нарушителю", как стремящемуся похитить какой-либо документ, установить подслушивающее устройство, так и "нарушителю", осуществляющему разбойное нападение или преследующего иные цели.

Исходя из анализа возможных "моделей" нарушителя, способов получения им информации, конкретной архитектуры здания, характеристик территории, прилегающих зданий, рельефа местности

и т.д., вырабатываются требования к инженерной защите, системе охранной сигнализации и размещению постов. Последнее означает, что для каждого конкретного объекта, здания, помещения должен разрабатываться конкретный проект его оснащения ТСОС-ТСН, СКД с учетом требований "Системной концепции...", дабы не допустить пробелов в системе защиты, которые раньше или позже но будут обнаружены грамотным злоумышленником.

Классификация нарушителей на основе моделей их действий (способов реализации угроз). Разработка моделей нарушителей осуществляется на основе исследования возможных видов угроз объекту и способов их реализации.

Угрозы могут носить общий или локальный характер и исходить:

- от людей (персонала, сторонних нарушителей или социальные, например: общественные беспорядки, забастовки и т.д.);
- от природных факторов (наводнение, засуха, землетрясение, снегопад, проливные дожди и т.д.);
- от нарушения систем жизнеобеспечения из-за техногенных факторов (отключение электропитания, пожар, утечка газов, радиоактивные осадки и т.д.), а также угрозы могут носить случайный характер.

При рассмотрении вопросов классификации нарушителей нас интересуют способы реализации угроз, исходящих от людей (злоумышленников).

Рассматривают три типа нарушителей - неподготовленный, подготовленный, квалифицированный и две группы способов реализации угроз (враждебных действий) - контактные, бесконтактные.

Способы проникновения на объект, в его здания и помещения могут быть самые различные (это описано во многих литературных источниках), например:

- разбитие окна, витрины, остекленной двери или других остекленных проемов;
- взлом (отжатие) двери, перепиливание (перекус) дужек замка и другие способы проникновения через дверь;
- пролом потолка, подлежащего блокировке;
- пролом капитального потолка, не подлежащего блокировке;
- пролом стены, подлежащей блокировке;
- пролом капитальной стены, не подлежащей блокировке;
- пролом (подкоп) капитального пола, не подлежащего блокировке;
- пролом (подкоп) пола, подлежащего блокировке;
- проникновение через разгрузочный люк;
- проникновение через вентиляционное отверстие, дымоход или другие строительные коммуникации;
- проникновение подбором ключей;
- оставление нарушителя на объекте до его закрытия;
- свободный доступ нарушителя на объект в связи с временным нарушением целостности здания из-за влияния природно-техногенных факторов или в период проведения ремонта;
- проникновение через ограждение (забор, сетку, решетку), используя подкоп, перелаз, разрушение, прыжок с шестом и т.д.

Очевидно, что каждый тип нарушителей (неподготовленный, подготовленный,

квалифицированный) будет осуществлять проникновение на объект по разному - менее грамотно или более грамотно (ухищренно), используя различные условия, способствующие проникновению, как то:

- взрыв;
- пожар (поджог);
- разбойное нападение;
- наводнение;
- химическое заражение;
- общественные беспорядки;
- отключение электроэнергии на объекте, в районе, городе;
- постановка нарушителем помех ТСО на объекте;
- постановка нарушителем помех в канале связи объекта с охраной;
- предварительный вывод из строя ТСО на объекте;
- предварительный вывод из строя канала связи объекта с охраной;
- предварительный сговор нарушителя с персоналом объекта;
- предварительный сговор нарушителя с персоналом службы охраны объекта;
- создание и использование многих и многих других условий для проникновения на охраняемый объект, например: использование дрессированных животных и птиц, специальных технических средств обхода ТСО, специальных технических средств для предварительного изучения объекта и т.д.

Ряд моделей действий нарушителей достаточно широко представлены в художественной литературе, кинофильмах, в телепередачах с криминальными сюжетами, в научно-технических изданиях в открытой печати. Таким образом, потенциальному злоумышленнику вполне доступно повышение квалификации на материалах открытой печати, телепередач и кино. Этот неоспоримый факт, безусловно, должна в своей деятельности учитывать СБ(О) и соответственно строить тактику охраны учреждения. Очевидно, информация о тактике охраны (способах и методах противодействия любым из возможных действий злоумышленника) является строго конфиденциальной, секретной и совершенно секретной.

В зависимости от поставленных целей злоумышленник создает те или иные условия для проникновения на объект и в его помещения, пользуясь теми или иными контактными или бесконтактными способами проникновения.

К контактным способам совершения враждебных действий относятся:

1. Контактное проникновение на объект охраны (ОО): несанкционированное проникновение на территорию ОО;
- проход на основе маскировки (под сотрудника ОО, посетителя и т.п.);
- установка (занос на ОО) средств негласного слухового, визуального, электромагнитного и др. наблюдения.
2. Контактное нарушение целостности или характера функционирования объекта:
- нарушение линий жизнеобеспечения ОО;
- физическая ликвидация потенциала (ресурсов) ОО (взрыв, разрушение и др.);
- затруднение штатного режима функционирования объекта.

К бесконтактным способам совершения враждебных действий относятся:

1. Бесконтактные проникновения на объект охраны:
- перехват физических полей;
- контроль радио- и телефонных переговоров;
- визуальное и слуховое наблюдение;
2. Вывод объекта из строя без проникновения на него, как то:
- нарушение целостности объекта посредством использования направленного взрыва или дистанционного оружия;
- отключение линий жизнеобеспечения объекта.

Нарушителем считается лицо, нарушающее контрольно-пропускной режим, случайно

или преднамеренно нарушающее режим безопасности объекта охраны.
Для описания моделей нарушителей в качестве критериев классификации рассматриваются:

1. Цели и задачи вероятного нарушителя:
- проникновение на охраняемый объект без причинения объекту видимого ущерба (для решения задач разведки объекта, установки техники, закладки других устройств и т.п.);
- причинение ущерба объекту (при этом проникновение - только промежуточная задача действий вероятного нарушителя);
- освобождение спецконтингента (арестованных);
- преднамеренное проникновение при отсутствии враждебных намерений (любопытство, проникновение при решении посторонней задачи и др.);
- случайное проникновение.
2. Степень принадлежности вероятного нарушителя к объекту:
- вероятный нарушитель - сотрудник охраны;
- вероятный нарушитель - сотрудник учреждения;
- вероятный нарушитель - постороннее лицо.
3. Степень осведомленности вероятного нарушителя об объекте:
- детальное знание объекта;
- осведомленность о назначении объекта, его внешних признаках и чертах;
- неосведомленный вероятный нарушитель.
4. Степень осведомленности вероятного нарушителя о системе охраны объекта:
- полная информация о системе охраны объекта;
- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;
- информация о системе охраны вообще, но не о системе охраны конкретного объекта;
- неосведомленный вероятный нарушитель.
5. Степень профессиональной подготовленности вероятного нарушителя:
- специальная подготовка по преодолению систем охраны;
- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.
6. Степень физической подготовленности вероятного нарушителя:
- специальная физическая подготовка;
- низкая физическая подготовка.
7. Владение вероятным нарушителем способами маскировки:
- вероятный нарушитель владеет способами маскировки;
- вероятный нарушитель не владеет способами маскировки.
8. Степень технической оснащенности вероятного нарушителя:
- оснащен специальной техникой для преодоления системы охраны;
- оснащен стандартной техникой;
- не оснащен техническими приспособлениями.
9. Способ проникновения вероятного нарушителя на объект:
- использование негативных качеств личного состава охраны объекта;
- "обход" технических средств охраны;
- движение над поверхностью земли;
- движение по поверхности земли (в том числе подкоп).

На основе изложенных критериев можно выделить четыре категории нарушителя:
- нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель- профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов (квалифицированный нарушитель);
- нарушитель второй категории - непрофессиональный нарушитель с враждебными

намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект (подготовленный нарушитель);
- нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;
- нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

В принципе под моделью нарушителя понимается совокупность количественных (вес, скорость перемещения, рост и т.п.) и качественных (цели и способы действия, степень осведомленности и подготовленности и т.п.) характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны (КИТСО) и/ или его составным частям.

Существуют определенные методики количественной оценки вероятностей обнаружения нарушителя, пытающегося проникнуть на объект охраны. Здесь учитываются гамма параметров, характеризующих категорию важности объекта, конфигурацию, архитектуру и тактико-технические характеристики применяемых в КТСО ТСОС, ТСН, СКД, а также количественных и качественных характеристик нарушителя и возможных моделей его действия.

Вопросы классификации угроз информационной безопасности. В системе обеспечения безопасности объектов одно из ведущих мест занимает обеспечение информационной безопасности. Действительно, любой (не случайный) потенциальный нарушитель до проникновения на объект и проведения преступных действий проводит в зависимости от поставленных им конечных целей более или менее глубокую разведку с тем, чтобы обезопасить себя и выполнить поставленную преступную задачу. Поэтому защита от посторонних лиц жизненно важной информации об объекте (количество и виды ресурсов, планы, уникальные технологии, места расположения жизненно важных центров обеспечения деятельности, например серверов баз данных, конструкторско-технологической документации и т.д.), а также информации о системе обеспечения охранной деятельности (структура, состав и режимы работы служб безопасности; структура, состав и принципы действия ТСО, СКД и т.д.; схемы размещения и принципы действия специальных технических средств обнаружения каналов утечки информации, обнаружения ДТС и т.д.) является наиболее приоритетной задачей, от успешного решения которой зависит уровень эффективности защиты объекта в целом.

Проблемы защиты информации решаются в каждом из блоков задач, рассматриваемых системной концепцией обеспечения комплексной безопасности объекта, и в каждом блоке эти проблемы решаются своими способами и методами, хотя имеются и некоторые общие особенности.

В каждом случае работа СБ(О) начинается с моделирования потенциальных угроз безопасности информации, их классификации и выбора (разработки) адекватных угрозам мер информационной защиты.

Рассмотрим для примера вопросы классификации угроз при решении проблем обеспечения безопасности автоматизированных систем обработки информации (АСОИ), т.е. ПЭВМ, ЛВС, серверов баз данных и т.д. и их информационного и программного обеспечения.

В большинстве случаев (например, в банковской деятельности около 80%) нарушения по НСД к АСОИ исходят от самих сотрудников учреждений. Потери в денежном выражении составляют от них около 70%, остальные потери приходятся на хакеров, террористов и т.п.

Можно выделить три основные причины внутренних нарушений: безответственность, самоутверждение и корыстный интерес пользователей (персонала) АСОИ [49]. Кроме того существуют угрозы, исходящие от хакеров и иных нарушителей извне.

Есть опасность нанесения ущерба и не по злому умыслу, когда сотрудник учреждения,

имеющий доступ к базам данных ЛВС или ПЭВМ обладает малой квалификацией, невнимателен, недисциплинирован, неряшлив в соблюдении технологии обработки информации или в пользовании программными продуктами, либо просто утомлен, омрачен какими-то личными переживаниями, что также приводит к невнимательности. При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Предусмотреть все такие ситуации маловероятно. Более того, во многих случаях система в принципе не может предотвратить подобные нарушения (например, случайное уничтожение своего собственного набора данных). Иногда ошибки поддержки адекватной защищенной среды могут поощрять такого рода нарушения. Система защиты может быть также неправильно настроена. Эти категории "нарушителей" в излагаемой книге специально не рассматриваются.

О самоутверждении. Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, ведя своего рода игру "пользователь - против системы" ради самоутверждения либо в собственных глазах, либо в глазах коллег. Хотя при этом намерения могут быть и безвредными, эксплуатация ресурсов АСОИ считается нарушением политики безопасности. Пользователи с "более криминальными намерениями" могут найти конфиденциальные данные, попытаться испортить или уничтожить их. Такой вид нарушений называется зондированием системы. Большинство систем имеет ряд средств противодействия подобным "шалостям".

Нарушение безопасности АСОИ может быть вызвано и корыстным "злоумышленником". Под "злоумышленником" понимается человек (извне или сотрудник), обладающий достаточными знаниями в вопросах автоматизированной обработки информации, преследующий цели сознательного воздействия, направленного на кражу секретной информации о деятельности учреждения, его планах, процедурах проведения операций, организации системы охраны и т.д., т.е. той информации, которая позволит злоумышленнику в конце концов осуществить кражу средств, материальных или финансовых, или дезорганизовать деятельность учреждения. В этом случае он целенаправленно пытается преодолеть систему защиты от несанкционированного доступа к хранимой, передаваемой и обрабатываемой в АСОИ информации. Полностью защититься от таких проникновений практически невозможно. В какой-то мере утешает лишь то, что опаснейшие нарушения встречаются крайне редко, ибо требуют необычайного мастерства и упорства от злоумышленника, и его злонамеренное действие при грамотно организованной системе контроля может быть обнаружено, т.е. вероятность проведения таких акций против АСОИ может быть существенно снижена.

Приведем некоторые данные о количестве и объеме угроз для безопасности со стороны корыстных злоумышленников.

Итальянские психологи утверждают, что из всех служащих любой фирмы 25% - это честные люди, 25% - ожидают удобного случая для разглашения секретов и 50% будут действовать в зависимости от обстоятельств [141].

В 1994 г. трое репортеров лондонской газеты "Санди Тайме" провели эксперимент. Представляясь бизнесменами, они вышли на двадцать депутатов британского парламента с предложением направить в правительство запрос, в котором они заинтересованы, и получить за это наличными или чеком тысячу фунтов стерлингов. Из двадцати 17 сразу отказались, трое согласились. Аналогичные эксперименты проводила ФБР в начале 80-х гг.: агенты ФБР под видом арабских шейхов обращались к членам американского конгресса, предлагая им вознаграждение в десятки тысяч долларов за то, чтобы "шейхам" были устроены всякие поблажки [183].

Если эти закономерности перенести, например, на банковских служащих, то более чем от 10% персонала можно ожидать неприятностей, связанных с продажей секретной информации.

Очевидно, ущерб от каждого вида нарушений зависит от частоты их появления и ценности информации. Чаще всего встречаются нарушения, вызванные халатностью и безответственностью, но ущерб от них обычно незначителен и легко восполняется. Например, во многих системах существуют средства, позволяющие восстанавливать случайно уничтоженные наборы данных при условии, что ошибка сразу же обнаружена. Регулярное архивирование рабочих файлов данных, имеющих важное значение, позволяет существенно уменьшить ущерб от их потери.

Ущерб от зондирования системы может быть гораздо больше, но и вероятность его во много раз ниже, ибо для таких действий необходимы достаточно высокая квалификация, отличное знание системы защиты и определенные психологические особенности. Наиболее характерным результатом зондирования системы является блокировка: пользователь вводит АСОИ в состояние неразрешимого противоречия (например, ввести задачу - софизм или вирус), после чего операторы и системные программисты тратят много времени для восстановления работоспособности системы. К примеру, в скандальной истории с вирусом Морриса в сети Internet, бывшей результатом зондирования системы, ущерб исчислялся миллионами долларов.

Отличительной чертой проникновений, наиболее редких, но и наиболее опасных нарушений, обычно является определенная цель: доступ (чтение, модификация, уничтожение) к определенной информации, влияние на работоспособность системы, слежение за действиями других пользователей и др. Для осуществления подобных действий нарушитель должен обладать теми же качествами, что и для зондирования системы, только в усиленном варианте, а также иметь точно сформулированную цель. Ущерб от проникновений может оказаться в принципе невосполнимым. Например, для банков это может быть полная или частичная модификация счетов с уничтожением журнала транзакций (полностью законченная операция с деньгами), т.е. если с какого-то счета сняты деньги, то они должны быть записаны в другом счете (не теряться и не быть излишками).

Причины, побуждающие пользователя совершать нарушения или даже преступления, различны. Наиболее серьезный ущерб системе угрожает в случае умышленного воздействия из-за обиды, неудовлетворенности своим служебным и/или материальным положением, или по указанию других лиц, под угрозой шантажа. Шантаж, как одно из средств нелегального доступа к ценной информации, используется преступными организациями, проводящими для этого специальные мероприятия по дискредитации ответственных работников учреждения. Ущерб при этом тем больше, чем выше положение пользователя в служебной иерархии.

Способы предотвращения ущерба в этом случае вытекают из природы причин (побудительных мотивов) нарушений и преступлений. Это - соответствующая подготовка пользователей, поддержание здорового рабочего климата в коллективе, подбор персонала, своевременное обнаружение потенциальных злоумышленников и принятие соответствующих мер. Ясно, что это не только задачи администрации и детективной группы, но и коллектива в целом. Сочетание этих мер способно предотвратить сами причины нарушений и преступлений.

Таким образом, наиболее уязвимым с позиции обеспечения безопасности может стать "человеческий фактор", т.е. недисциплинированность сотрудников, недостаточный профессионализм, возможность подкупа, шантажа, угроз насилия, обиды по поводу неадекватной оценки труда и многое другое. Более детальное описание методов противодействия такого рода угрозам изложены, например, в [27]. Отметим лишь, что коль скоро такие угрозы существуют, следует рекомендовать проведение соответствующих тщательных исследований детективной группой, отделом кадров и администрацией с привлечением профессиональных психологов, психоаналитиков, педагогов и соответствующих технических средств (например, многофункциональных детекторов лжи).

Очевидно, что для выбора оптимального варианта нейтрализации действий злоумышленника из известных методов, способов и средств противодействия нужно знать (либо предполагать), что собой представляют (либо могут представлять) возможные нарушения и злоумышленник, т.е. нужны модели нарушений, "модель" нарушителя или "модель" его возможных действий. Исследование моделей нарушителей является отправной идеей в разработке стратегии и тактики обеспечения безопасности АСОИ. В самом деле, для выбора средств защиты нужно ясно представлять, от кого защищать АСОИ.

Например, возможен такой подход: на основе доступности компонентов программного и информационного обеспечения в табл. 1.1 представлены типы угроз и лица, которые могли бы вызвать такие угрозы.

При создании модели нарушителя и оценке риска потерь от действий персонала (необходимых этапов выработки политики безопасности) дифференцируют всех сотрудников по их возможностям доступа к системе и, следовательно, по потенциальному ущербу от каждой категории пользователей. Например, оператор или программист автоматизированной банковской системы может нанести несравненно больший ущерб, чем обычный пользователь, тем более непрофессионал.

Таблица 1.1. **Типы угроз и возможных нарушителей**

Тип угрозы	Нарушитель				
	Оператор	Сотрудник из управления	Программист	Инженер по техническому обслуживанию	Пользователь
Изменение кодов	+		+		
Копирование файлов	+		+		
Уничтожение файлов	+	+	+		+
Присвоение программ			+		
Шпионаж	+	+	+	+	
Установка подслушивания			+	+	
Саботаж	+		+		
Продажа данных	+	+	+		+
Воровство			+	+	+

Приведем примерный список персонала типичной АСОИ и соответствующую степень риска от каждого из них [46; 49]:

1. Наибольший риск:
- системный контролер;
- администратор безопасности.
2. Повышенный риск:
- оператор системы;
- оператор ввода и подготовки данных;
- менеджер обработки;
- системный программист.
3. Средний риск:
- инженер системы;
- менеджер программного обеспечения.
4. Ограниченный риск:
- прикладной программист;

- инженер или оператор по связи;
- администратор баз данных;
- инженер по оборудованию;
- оператор периферийного оборудования;
- библиотекарь системных магнитных носителей;
- пользователь-программист;
- пользователь-операционист.

5. Низкий риск:
- инженер по периферийному оборудованию;
- библиотекарь магнитных носителей пользователей.

Итак, при проектировании системы защиты АСОИ следует уделять внимание не только возможным объектам нарушений, но и вероятным нарушителям как личностям. Многолетний опыт функционирования тысяч АСОИ свидетельствует, что совершаемые без причины, а в силу случайных обстоятельств преступления очень редки.

На основе изложенных пояснений сути рассматриваемой проблемы моделирования угроз, нарушителей и их действий можно предложить следующий подход к классификации угроз безопасности АСОИ.

Отметим, что попытки дать исчерпывающую классификацию угроз безопасности АСОИ предпринимались неоднократно, однако список их постоянно расширяется, и потому в данном учебном пособии выделим лишь основные их типы.

Проводимая ниже классификация охватывает только умышленные угрозы безопасности АСОИ, оставляя в стороне такие воздействия как стихийные бедствия, сбои и отказы оборудования и др. Реализацию угрозы принято называть атакой.

Угрозы безопасности можно классифицировать по следующим признакам (выделим 9 групп) [27]:

1. **По цели реализации угрозы.** Атака может преследовать следующие цели:
- нарушение конфиденциальности информации;
- нарушение целостности информации (ущерб от уничтожения или несанкционированной модификации информации может быть много больше, чем при нарушении конфиденциальности);
- нарушение (полное или частичное) работоспособности АСОИ (нарушение доступности). Такие нарушения могут повлечь за собой неверные результаты, отказы от обработки потока информации или отказы при обслуживании.

2. **По принципу воздействия на АСОИ:**
- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.);
- с использованием скрытых каналов.

Субъектом доступа называется лицо или процесс, действия которого регламентируются правилами разграничения доступа, а объектом доступа - единица информационного ресурса АСОИ, доступ к которой регламентируется правилами разграничения доступа.

Под доступом понимается взаимодействие между субъектом и объектом (выполнение первым некоторой операции над вторым), приводящее к возникновению информационного потока от второго к первому.

Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимосвязанным процессам обмениваться информацией таким способом, который нарушает системную политику безопасности (способ управления доступом). Скрытые каналы бывают двух видов:
- скрытые каналы с памятью, позволяющие осуществлять чтение или запись информации другого процесса непосредственно или с помощью промежуточных объектов для хранения информации (временной памяти);
- скрытые временные каналы, при которых один процесс может получать информацию о действиях другого, используя интервалы между какими-либо событиями (например,

анализ временного интервала между запросом на ввод-вывод и сообщением об окончании операции, что позволяет судить о размере вводимой или выводимой информации).

3. **По характеру воздействия на АСОИ.** Различают активное и пассивное воздействие. Первое всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к наборам данных, программам, вскрытие пароля и т.д.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализа. Пример - прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации в АСОИ, так как при нем никаких действий с объектами и субъектами не производится.

4. **По факту наличия возможной для использования ошибки защиты.** Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты.

Такая ошибка может быть обусловлена одной из следующих причин:

- неадекватностью (несоответствием) политики безопасности реальной АСОИ. В той или иной степени несоответствия такого рода имеют все системы, но в одних случаях это может привести к нарушениям, а в других - нет. Если выявлена опасность такого несоответствия, необходимо усовершенствовать политику безопасности, изменив соответственно средства защиты;
- ошибками административного управления, под которыми понимают некорректную реализацию или поддержку принятой политики безопасности в данной АСОИ. Пусть, например, согласно политике безопасности в АСОИ должен быть запрещен доступ пользователей к некоторому определенному набору данных, а на самом деле (по невнимательности администратора безопасности) этот набор данных доступен всем пользователям. Обнаружение и исправление такой ошибки требуют обычно небольшого времени, тогда как ущерб от нее может быть огромен;

ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программ или комплекса программ и из-за которых эти программы могут быть использованы совсем не так, как описано в документации. Такие ошибки могут быть очень опасны, к тому же их трудно найти, а для устранения надо менять программу или комплекс программ;

- ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапах реализации, отладки и могут служить источником недокументированных свойств.

5. **По способу воздействия на объект атаки (при активном воздействии):**

- непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа;
- воздействие на систему разрешений (в том числе захват привилегий). При этом несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом;
- опосредованное воздействие (через других пользователей):
- "маскарад". В этом случае пользователь присваивает себе каким-либо образом полномочия другого пользователя, выдавая себя за него;
- "использование вслепую". При таком способе один пользователь заставляет другого выполнить необходимые действия (для системы защиты они не выглядят несанкционированными, ибо их выполняет пользователь, имеющий на это право), причем последний о них может и не подозревать. Для реализации этой угрозы может использоваться вирус (он выполняет необходимые действия и сообщает о их результате тому, кто его внедрил).

Два последних способа очень опасны. Для предотвращения подобных действий требуется постоянный контроль как со стороны администраторов и операторов за работой АСОИ в целом, так и со стороны пользователей за своими собственными наборами данных.

6. **По способу воздействия на АСОИ:**

- в интерактивном режиме;
- в пакетном режиме.

Работая с системой, пользователь всегда имеет дело с какой-либо ее программой. Одни программы составлены так, что пользователь может оперативно воздействовать на ход их выполнения, вводя различные команды или данные, а другие так, что всю информацию приходится задавать заранее. К первым относятся, например, некоторые утилиты, управляющие программы баз данных, в основном - это программы, ориентированные на работу с пользователем. Ко вторым относятся в основном системные и прикладные программы, ориентированные на выполнение каких-либо строго определенных действий без участия пользователя.

При использовании программ первого класса воздействие оказывается более длительным по времени и, следовательно, имеет более высокую вероятность обнаружения, но более гибким, позволяющим оперативно менять порядок действий. Воздействие с помощью программ второго класса (например, с помощью вирусов) является кратковременным, трудно диагностируемым, гораздо более опасным, но требует большой предварительной подготовки для того, чтобы заранее предусмотреть все возможные последствия вмешательства.

7. **По объекту атаки.** Объект атаки - это тот компонент АСОИ, который подвергается воздействию со стороны злоумышленника. Воздействию могут подвергаться следующие компоненты АСОИ:

- АСОИ в целом: злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Используют обычно "маскарад", перехват или подделку пароля, взлом или доступ к АСОИ через сеть;

объекты АСОИ - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности (например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения (нарушение доступности АСОИ);

- субъекты АСОИ - процессы и подпроцессы пользователей. Целью таких атак является либо прямое воздействие на работу процессора - его приостановка, изменение характеристик (например, приоритета), либо обратное воздействие - использование злоумышленником привилегий, характеристик другого процесса в своих целях. Воздействие может оказываться на процессы пользователей, системы, сети;
- каналы передачи данных. Воздействие на пакеты данных, передаваемые по каналу связи, может рассматриваться как атака на объекты сети, а воздействие на сами каналы - как специфический род атак, характерный для сети. К последним относятся: прослушивание канала и анализ графика (потока сообщений); подмена или модификация сообщений в каналах связи и на узлах- ретрансляторах; изменение топологии и характеристик сети, правил коммутации и адресации.

8. **По используемым средствам атаки.** Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ АСОИ хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но

может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавления программ в АСОИ без разрешения администратора безопасности системы.

9. **По состоянию объекта атаки.** Состояние объекта в момент атаки весьма существенно для результатов атаки и содержания работы по ликвидации ее последствий. Объект атаки может находиться в одном из трех состояний:

- хранения на диске, магнитной ленте, в оперативной памяти или в любом другом месте в пассивном состоянии. При этом воздействие на объект обычно осуществляется с использованием доступа;
- передачи по линии связи между узлами сети или внутри узла, Воздействие предполагает либо доступ к фрагментам передаваемой информации (например, перехват пакетов на ретрансляторе сети), либо просто прослушивание с использованием скрытых каналов;
- обработки в тех ситуациях, когда объектом атаки является процесс пользователя.

Приведенная классификация показывает сложность определения возможных угроз и способов их реализации.

Более подробно распространенные угрозы безопасности АСОИ рассмотрены, например, в [18].

В связи с тем, что универсального способа защиты, который мог бы предотвратить любую угрозу, не существует, для обеспечения безопасности АСОИ в целом создают защитную систему, объединяя в ней различные меры защиты.

Изложенный далеко не полно пример решения проблемы классификации угроз информационной безопасности АСОИ убеждает в необходимости проведения глубоких исследований при решении аналогичных проблем в контуре всех иных блоков задач "Системной концепции..." [100].

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы по дисциплине «**Гуманитарные проблемы обеспечения информационной безопасности**»

для студентов направления подготовки 10.03.01 Информационная безопасность

направленность (профиль) Безопасность компьютерных систем

Пятигорск, 2024

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

− формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

− написание докладов;

− подготовка к семинарам, практическим и лабораторным работам, их оформление;

− составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

− выполнение учебно-исследовательских работ, проектная деятельность;

− подготовка практических разработок и рекомендаций по решению проблемной ситуации;

− выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

− компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

− выполнение курсовых работ (проектов) в рамках дисциплин;

− выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

● подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

● основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

● заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Гуманитарные проблемы обеспечения компьютерной безопасности» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ОПК-1. Способен оценивать роль информации,	ИД-1 ОПК-1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах. ИД-2 ОПК-1 Способен администрировать средства защиты

информационных технологий и информационной безопасности в современной обществе, их значения для обеспечения объективных потребностей и личности, общества и государства	информации в компьютерных системах и сетях. ИД-3 ОПК-1 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям. ИД-4 ОПК-1 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями..

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

● систематизация и закрепление полученных теоретических знаний и практических умений студентов;

● углубление и расширение теоретических знаний;

● формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

● развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

● формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

● развитие исследовательских умений;

● использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (акад.)		
			СРС	Контактная	Всего

				работа с преподавателем	
3 семестр					
ОПК-1, ПК-3	Самостоятельное изучение литературы и источников	Собеседование	16,92	1,88	18,8
ОПК-1, ПК-3	Подготовка к лабораторным занятиям	Опрос	6,48	0,72	7,2
ОПК-1, ПК-3	Написание реферата/доклада	Доклад	9	1	10
Итого за 3 семестр			**32,4**	**3,6**	**36**

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим

собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то

появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно,

исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;

● шрифт Times New Roman;

● кегль шрифта 14;

● межстрочное расстояние 1,5;

● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;

● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент	Обнаруживает недостаточное владение навыками работы с техническими	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	средствами и соответствующими и информационными технологиями		(более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные поручения в групповом проекте.	Проект не сдан.

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению

знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Современные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / И.А. Королькова / А.Р. Ванютин / А.П. Алексеев ; ред. А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. - 101 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Адлер, Ю.П. Статистическое управление процессами. «Большие данные» Электронный ресурс : учебное пособие / Е.А. Черных / Ю.П. Адлер. - Статистическое управление процессами. «Большие данные»,2021-09-01. - Москва : Издательский Дом МИСиС, 2016. - 52 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-87623-969-3, экземпляров неограниченно

Дополнительная литература:

1. Современные информационные технологии Электронный ресурс : Сборник трудов по материалам 3-й межвузовской научно-технической конференции с международным участием 29 сентября 2017 г. / В. И. Воловач [и др.] ; ред. В. М. Артюшенко. - Королёв : Научный консультант, МГОТУ, 2017. - 191 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-9500999-7-7, экземпляров неограниченно

2. Современные мультимедийные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / А.П. Алексеев / А.Р. Ванютин / И.А. Королькова. - Современные мультимедийные информационные технологии,2021-05-25. - Москва : СОЛОН-ПРЕСС, 2017. - 108 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-91359-219-4, экземпляров неограниченно

Методическая литература:

1. Методические рекомендации для самостоятельной работы студентов по дисциплине «Гуманитарные проблемы обеспечения компьютерной безопасности»

2. Методические указания к практическим работам по дисциплине «Гуманитарные проблемы обеспечения компьютерной безопасности»

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Гуманитарные проблемы обеспечения компьютерной безопасности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.