

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шебзухова Татьяна Александровна
Должность: Директор Пятигорского института (филиал) Северо-Кавказского
федерального университета
Дата подписания: 23.08.2023 15:53:29
Уникальный программный ключ:
d74ce93cd40e39275c3ba2f58486412a1c8ef96f

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
2022

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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 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	Объем часов	Из них практическая подготовка, часов
3 семестр			
1	Тема 1. Информационное общество. Информационная реальность. Методика построения матрицы состояний информационной безопасности	1,5	1,5

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

2	Тема 2. Гуманитарные проблемы формирования информационного общества. Действия органов и должностных лиц по предупреждению разглашения конфиденциальной информации	1,5	1,5
3	Тема 3. Понятие информационной безопасности. Работа с нормативно-правовыми документами, регламентирующими вопросы правового	1,5	1,5
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	1,5	1,5
5	Тема 5. Угрозы информационной безопасности на объекте. Юридические меры охраны конфиденциальных сведений как составная часть корпоративной системы защиты информации	1,5	1,5
6	Тема 6. Информационная безопасность как гуманитарная. Разработка инструкции по обеспечению сохранности конфиденциальной информации на предприятии	1,5	1,5
7	Тема 7. Принципы комплексной системы защиты информации. Организация службы безопасности предприятия	1,5	1,5
8	Тема 8. Методы и средства защиты информации. Системный подход к разработке концепции обеспечения безопасности информационного объекта	1,5	1,5
	Тема 9. Научные исследования в области информационной. Аналитический подход к классификации угроз безопасности информационного объекта на основе моделирования нарушителей и их действий	1,5	1,5
	Итого за 3 семестр	13,5	
	Итого	13,5	

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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 защиты, 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 конфиденциального 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. Основным 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. Назначение систем защиты информации

Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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

- Защита информационных и физических объектов информационных систем;
- Техническая защита информации на объектах ИС;
- Защита 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.

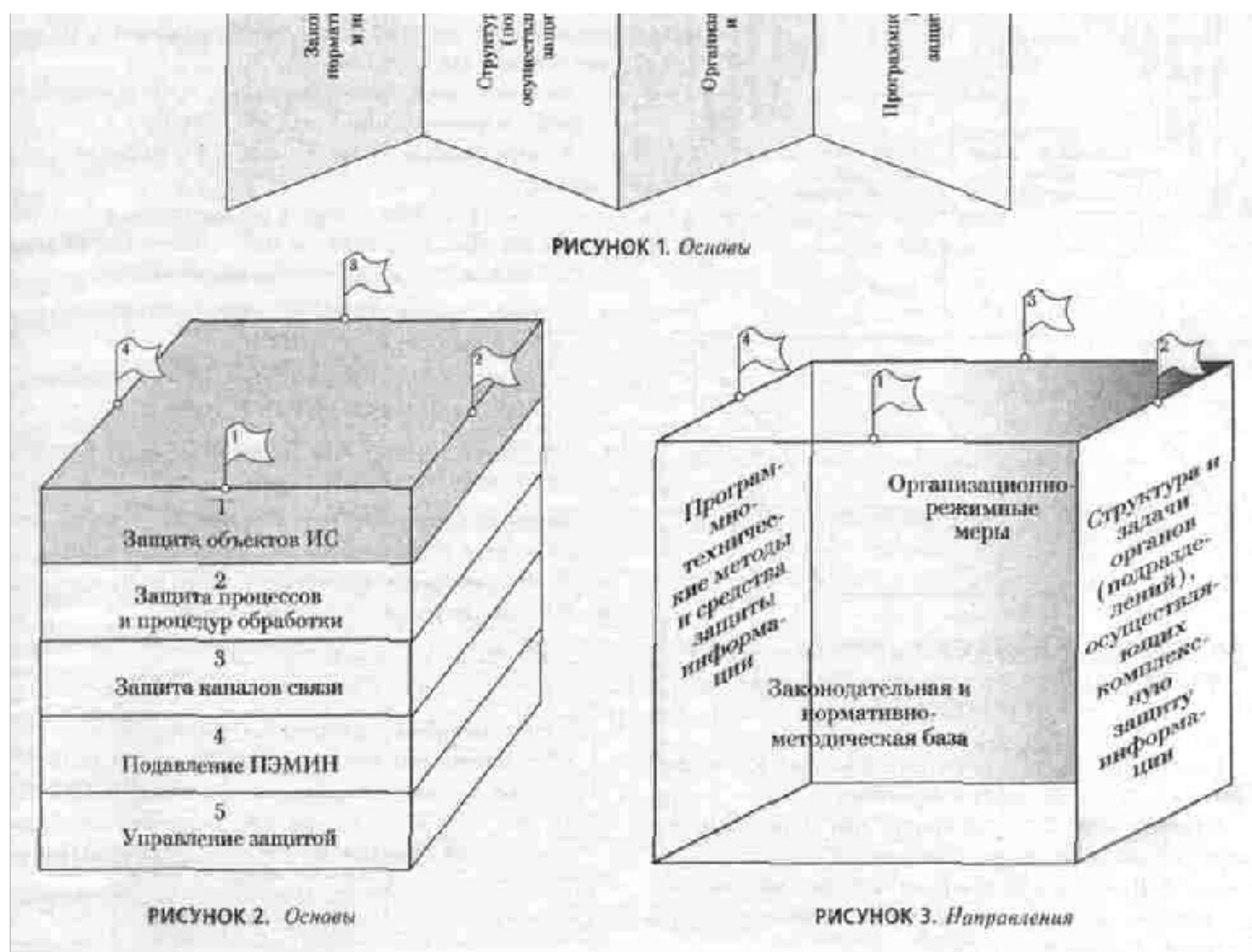
3. Этапы создания систем защиты информации

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.



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**).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022



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				ПЗМ и Н				Управление системой защиты			
		Базы	Структура	Меры	Средства	Базы	Структура	Меры	Средства	Базы	Структура	Меры	Средства	Базы	Структура	Меры	Средства	Базы	Структура	Меры	Средства
	Основы >>>	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

K — 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 $K = 4 * 5 * 7 = 140$

Представление элементов матрицы

Содержание каждого из элементов МАТРИЦЫ описывает взаимосвязь составляющих создаваемых вопросов описывающих каждый из элементов матрицы,

Сертификат 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Комплексное проектирование, создание и оценки СЗИ рассматривается путем анализа различных групп элементов матрицы, в зависимости от решаемых задач.

Действителен: с 20.08.2021 по 20.08.2022

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				ТСМ и И				Управление системой защиты			
		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 уязвимостей 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 выбранного 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				ТСМ и И				Управление системой защиты			
		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 уязвимостей 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 выбранного 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				ТСМ и И				Управление системой защиты			
		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 уязвимостей 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 выбранного 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:

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

РИСУНОК 10

Этапы >>>	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМ и Н				Управление системой защиты			
		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 и 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 ИС?

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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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, распространении и других способах обмена деловой и научной информацией.

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

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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



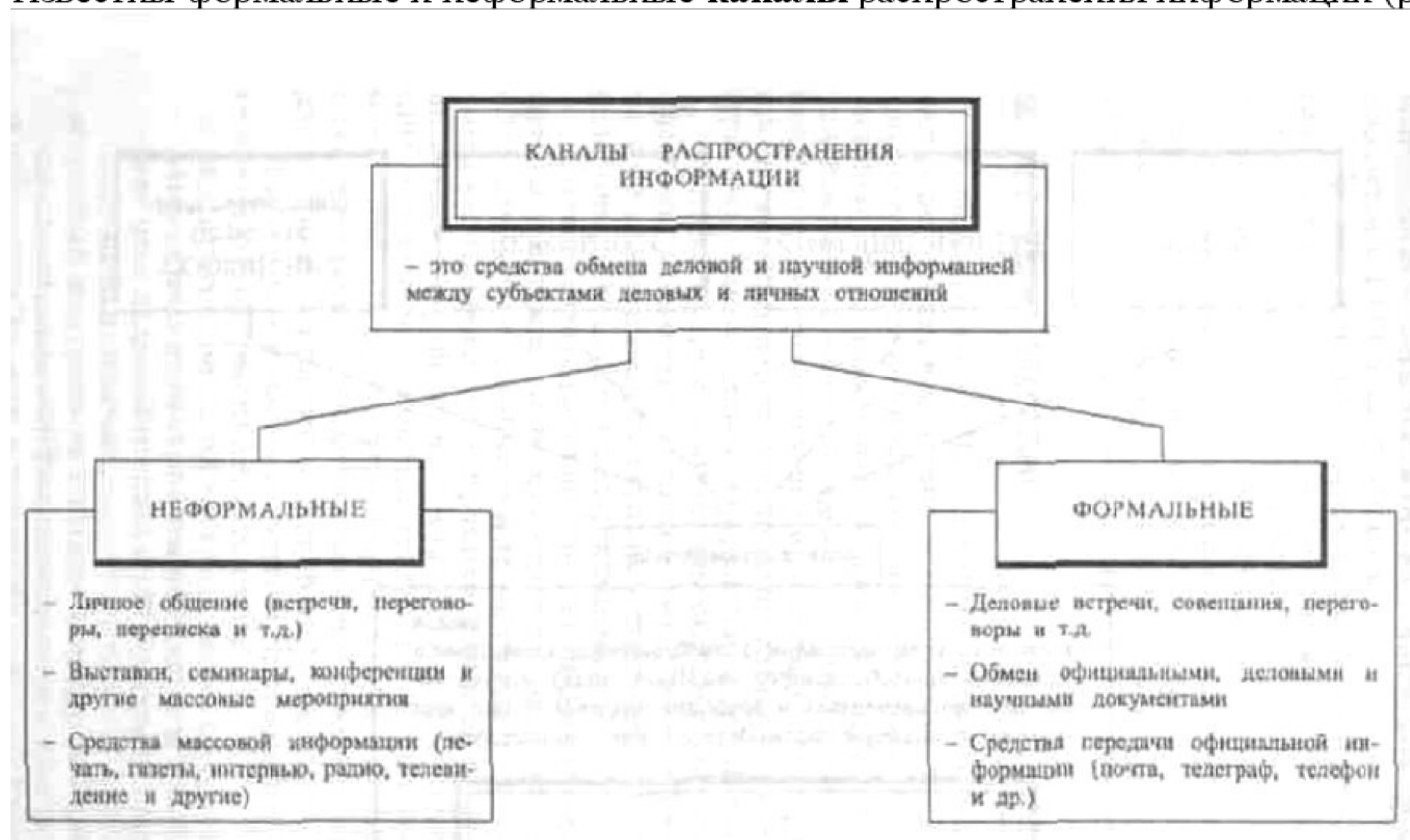
Разглашение конфиденциальной информации возможно:

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 **ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
Сертификат: 42000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
6. При **утрате документов:**
Действителен: с 20.08.2021 по 20.08.2022

- 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.

В основу защиты информации от разглашения целесообразно положить:

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 конкретного работника в сохранении тайны.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

является работа с кадрами, воспитательно-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 классификатора защитных действий по конфиденциальной информации. Такой документ может быть 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 из 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 методы 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-акустический контроль разговоров в служебных помещениях.

Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

Документ подписан ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Понимая всю важность соблюдения конфиденциальности мониторинга телефонных переговоров в пределах конкретного предприятия, Правительством РФ 22 марта 1995 г. Указом № 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 фонограммы 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 делопроизводства.
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. Петров 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 II. 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. Митрошин. Обеспечение информационной безопасности предприятия: Учебно-методическое пособие. М.: Городец, 2021. -192 с.

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

8. Брусилов Н.А. Открытость и шпионаж. - М.: Воениздат, 2013-56с.

9. Митрошин В.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".

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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 резмигрантов к государственной тайне" (утв. постановлением Правительства РФ от 22 августа 1998 г. N

1003) ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

2. Привести примеры исследовательского подхода к изучению дисциплины.

3. Дать примеры моральной 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 полномочия 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, и стремятся в установленном порядке получить лицензию на

ДОКУМЕНТ ПОДПИСАН

ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен с 20.08.2021 по 20.08.2022

Федеральным законом от 6 октября 1997 г. N 131-ФЗ установлен особый порядок допуска к государственной тайне членов Совета Федерации, депутатов 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

ДОКУМЕНТ ПОДПИСАН

ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

от 16 марта 1999 г. N 83

Действителен: с 20.08.2021 по 20.08.2022

Перечень медицинских противопоказаний для осуществления работы с использованием сведений, составляющих государственную тайну, утвержден приказом Минздрава РФ

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

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 заграничного плавания 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 или третьей форме, причины увеличения или снижения числа указанных должностей в новой номенклатуре.

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Номенклатура должностей работников

Действителен: с 20.08.2021 по 20.08.2022

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 указаный 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.

ДОКУМЕНТ ПОДПИСАН

II. ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Получение материалов на граждан, оформляемых (переоформляемых) на допуск к особой важности, совершенно секретным и секретным сведениям, осуществляется

управлением (отделом) 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 государственной
документ подписан
номенклатурный номер
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
допуска, дата окончания проведения проверочных мероприятий и наименование органа
Действителен с 20.08.2021 по 20.08.2022 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 **ДОКУМЕНТ ПОДПИСАН** на соответствующие должности.

Решение **ЭЛЕКТРОННОЙ ПОДПИСЬЮ** руководителей организаций, действующих в сфере ведения федеральных органов государственной власти, к государственной тайне принимается высшестоящими руководителями. В подразделения по защите государственной тайны этих

Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

организации 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.

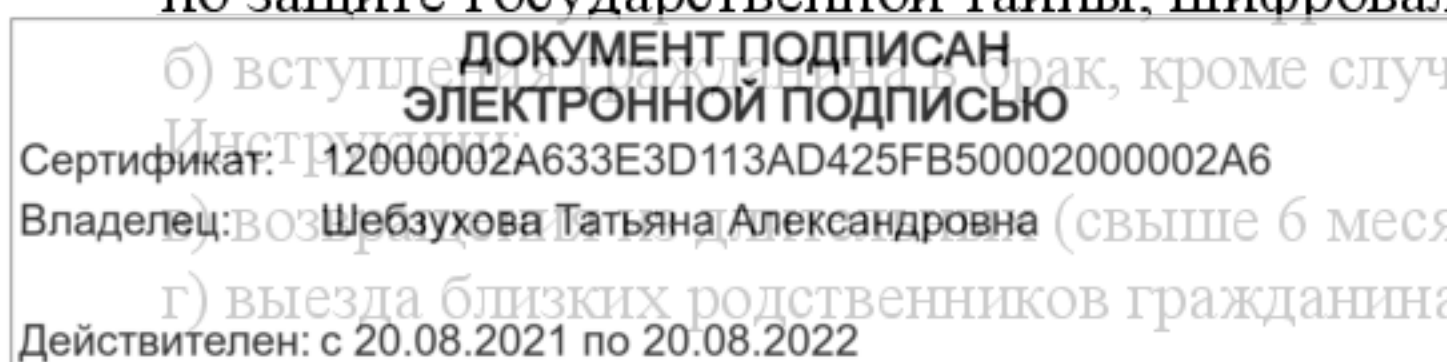
30. Переоформление допуска по первой или второй форме независимо от сроков действия производится в случае:

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

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

в) 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

проверочный документ

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебухова Татьяна Александровна

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

Действителен: с 20.08.2021 по 20.08.2022

особой важности, совершенно секретным и секретным сведениям при командировании и их в другие организации

в организациях, куда они командировются 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.

Исключением является случай, когда указанное лицо при выполнении задания неизбежно будет иметь доступ к сведениям особой важности или совершенно секретным сведениям.

Руководитель организации и подразделения 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

Исключением является случай, когда указанное лицо при выполнении задания неизбежно будет иметь доступ к сведениям особой важности или совершенно секретным сведениям.
Руководитель организации и подразделения 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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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 командированное 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.

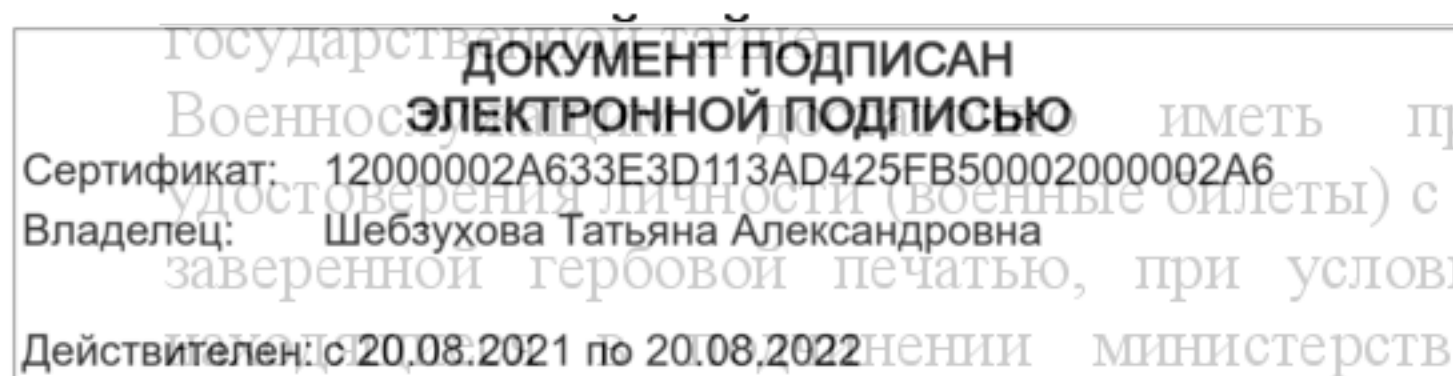
41. Командированное лицо может иметь доступ только к тем особой важности, совершенно секретным и секретным сведениям, которые ему необходимы в рамках выполняемого задания, указанного в предписании на выполнение задания (форма 16). Доступ осуществляется с письменного разрешения руководителя принимающей 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



иметь предписания на выполнение заданий и удостоверения личности (военные билеты) с отметкой о допуске к государственной тайне, при условии их командирования в воинские части, или их командирования в воинские части, или в 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 заграничного плавания 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

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен:	с 20.08.2021 по 20.08.2022

Закон Российской Федерации "О государственной тайне"
2. Постановление Правительства РФ от 28 октября 1995 г. N 1050 "Об утверждении
лищ 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., Шабаева А.Г. М.: Концерн "Банковский деловой центр", 2014. - 472 с.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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

Введение

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.

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 качествам в наибольшей степени соответствует требованиям данного рабочего места.

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

Вопрос 1. Метaproгpаммы в подборе и оценке персонала

Шебзухова Татьяна Александровна

Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2017 по 20.08.2022

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 особым 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,

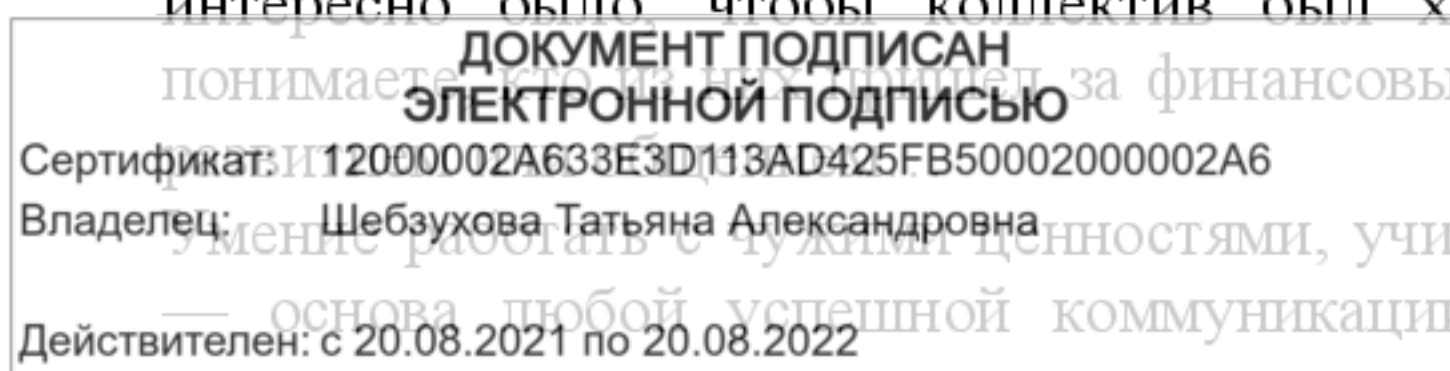
я задумалась — не представляющая интереса (машиной я пока не занимаюсь) информация в памяти не хранилась. Потом, заинтересовавшись, на расстоянии четырех автобусных остановок я обнаружила три магазина, где были представлены всевозможные автодетали. Так устроено наше внимание — оно выбирает то, что ценно 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 заинтересован в материальном результате, а кто — за самореализацией,

кто работает с чужими ценностями, учитывайте 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 — рефлексивность

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 рефлексивного типа предпочитают сначала размышлять, потом действовать. Они словно бы экономят энергию.

И как же нам по собеседованию определить активного и рефлексивного? 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...» Рефлексивный 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 рефлексивности.

Представим эту метапрограмму в виде шкалы:

Крайние значения (активный «мотор» или рефлексивный «тормоз») встречаются довольно редко. Но предпочтения определить все-таки можно. Статистики подсчитали, что граждан рефлексивного 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 рефлексивность: «не высывайся» (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 рефлексивный. Другой вопрос

— на каких должностях, куда, где нужно быстро действовать по ситуации (например торговый представитель, менеджер, руководитель), полезно набирать

активных. А в работе финансового аналитика, бухгалтера, эксперта лучше не торопиться — здесь как раз подойдут рефлексивные сотрудники.

Рассмотрим еще некоторые метапрограммы.

ДОКУМЕНТ ПОДПИСАН	
ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Щебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

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 — являются для человека более важными.

Есть люди, которые, говоря и всеми мыслями выражают внимание к себе, а другие, наоборот, выслушивают, вы понимают, 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 развеяться 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 попадая». 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 ажиотажа начала 1990-х годов, когда в страну стали массово

привозить тесты, а, вернее, краденые западные тесты, HR-ы столь же массово от них отказались. Стышком много подделок, а значит, бесполезных впусую.

Сейчас тесты отвоевывают позиции. Иногда этому способствуют экономические

Документ подписан
Электронной подписью
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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 – брендовых 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. В этой группе – знаменитый опросник MMPI (Minnesota Multiphasic

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен с 20.08.2021 по 20.08.2022

Personality Inventory), который HR-специалисты обычно вспоминают первым. Дают представление о индивидуальных 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 нелегальным 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 почтав 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 известен». И действительно, КОТ можно было не беспокоиться». Тест находится «на границе» интеллектуальных методик и тестов способностей. Позволяет оценить скорость и логику мышления, внимательность, получить представление о базовом уровне развития личности. 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 – чувство; 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 свидания. 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 объемный (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

характеристики личности и психическое состояние испытуемого.

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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 – АМТ (тесты для руководителей высшего звена), CRTB (анализ информации), MGIB (тесты для менеджеров).

На 90 вопросов ОРQ (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 Вyrковский Источник: Секрет Фирмы, 2014г.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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 меры защиты информации не могут физически схватить за руку злоумышленника или предотвратить его доступ к информации. Юридические средства выполняют особые функции, занимая 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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Преемственность законодательства. 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 законодательством, с которыми заключается трудовой договор на

Судебного суда РФ в своем постановлении от 17.03.04 №
Внимание. И если работник обратится в суд
или Рострудинспекцию с жалобой на неправомерность ваших действий, договор может
Действителен: с 20.08.2021 по 20.08.2022

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.

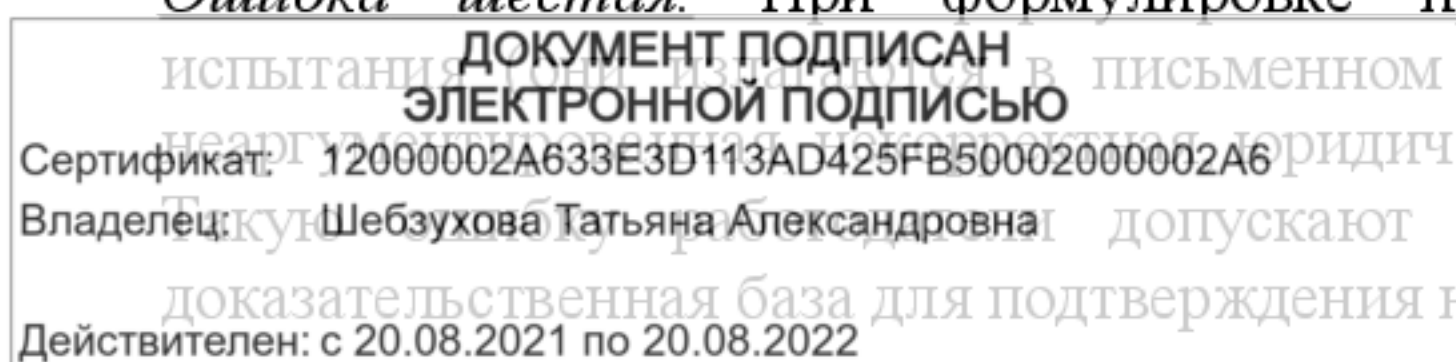
Ошибка четвертая. Здесь речь пойдет не об одной ошибке, а сразу о нескольких. Они напрямую связаны с невнимательным прочтением правил и установок, четко прописанных в нормах трудового права. Так, нередки случаи, когда испытание устанавливается для лиц, по закону освобожденных от предварительной проверки 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 работника в письменном виде и вручаются работнику) допускается юридически несостоятельная форма изложения.

Вследствие того, что у них отсутствует документальное подтверждение 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.

Выполняет документ подписан внутри объектного режима: исключая возможность
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
При ведении деловых переговоров с представителями сторонних организаций или
Действителен: с 20.08.2021 по 20.08.2022

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.: Юрист, 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

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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 открытых источниках информации, радио и телевидению, оглашение на международных, зарубежных и открытых внутрироссийских симпозиумах, совещаниях, конференциях, съездах, при публичных выступлениях и защите диссертаций, вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным

Документ подписан
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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 с партнерами - партнерами.

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

И ОБОЗНАЧЕНИЕ ДОКУМЕНТОВ, 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,

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
На зарегистрированном документе с грифом "КТ" своевременно отражается в журналах или карточках.
Действителен: с 20.08.2021 по 20.08.2022

Документы, которые не подшиваются в дела, своевременно отражаются 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" производится 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".

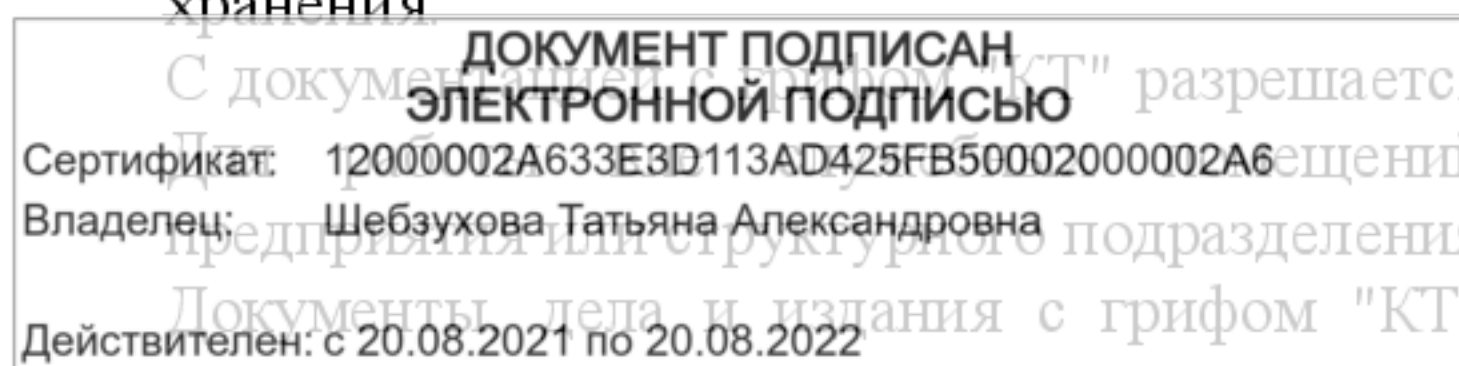
Снятия рукописных, машинописных, микро - и фотокопий, электрографических и др. копий, а также производство выписок из документов и изданий с грифом "КТ" сотрудниками предприятия производится по разрешению руководителя предприятия и подразделений.

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 документами с грифом "КТ" разрешается работать только в служебных помещениях. Для выписки или структурного подразделения необходимо разрешение руководителя.

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 на 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."

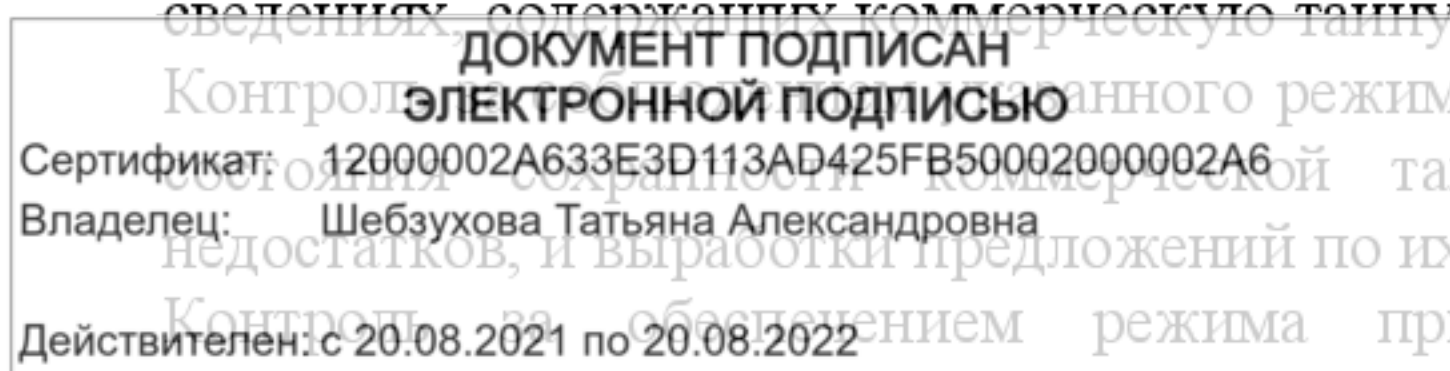
Дела и издания непосредственно представителям сторонних организаций и частным лицам не выдаются. При необходимости с их содержанием они знакомятся только с разрешения руководителя предприятия через уполномоченного службы безопасности или представителя заинтересованного подразделения.

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 выполнением внутриобъектового режима осуществляется в целях изучения и оценки соблюдения требований режима 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.

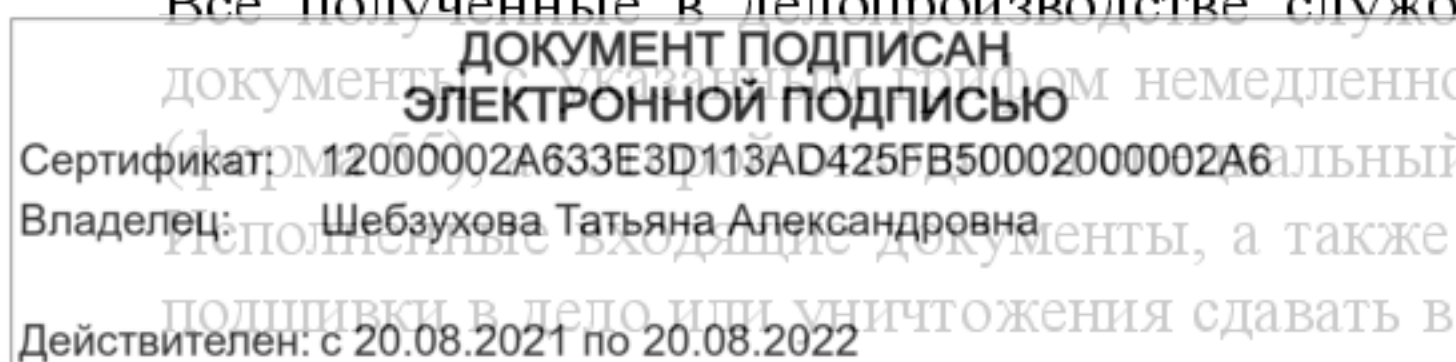
Предъявлять для проверки по требованию представителей службы безопасности все числящиеся документы с грифом "КТ", а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения.

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 немедленно вносить во внутреннюю опись документов (формы № 1 и № 2) и вносить в раздел по учету "КТ".

Исполнительные входящие документы, а также документы, предназначенные для рассылки, подписки в дело или уничтожения сдавать в делопроизводство службы безопасности или



уполномоченному службы безопасности.

Выполнять требования внутри объектного режима: исключая 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 сведений, составляющих коммерческую тайну предприятия

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

В настоящем перечне указываются категории не секретных 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 и фактические показатели финансирования капитальных вложений, научно-технических работ и затрат на внедрение новой техники

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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 не могут считаться конфиденциальными.

Сведения, раскрывающие существо позиции предприятия при ведении судебных и арбитражных дел за границей, разглашение которых может нанести ущерб предприятию.

9. ПОЛОЖЕНИЕ О СЛУЖБЕ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Сертификат:

12000002A633E3D113AD425FB5000200002A6

Владелец:

Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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, печатей, штампов предприятия, а также индивидуальных учетными номерами.

По вопросам делопроизводства:

Организует делопроизводство; контролирует обеспечение установленного порядка

Документ подписан	
ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

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 заграникомандировок.

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 подборе материалов, подготовленных к открытой публикации (статьи,

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

руководство уполномоченными по защите коммерческой тайны в структурных подразделениях. Проводит консультации для