МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_11_» _04_ 2023 г.

Гуманитарные аспекты информационной безопасности

Методические указания по организации самостоятельной работы по дисциплине «Планирование и управление информационной безопасностью» для студентов направления подготовки 10.03.01 и специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Гуманитарные аспекты информационной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 57 с.: Библиогр.: с. 57.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов для студентов направления подготовки 10.03.01 и специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Текст печатается в авторской редакции
Подписано в печать . Формат 60x84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ 228
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. **Задачи дисциплины:**

1. Формирование требований и проектирование системы управления ИБ.
2. Эффективное управление ИБ.
3. Сформировать у студентов практические навыки анализа и оценки гуманитарных аспектов информации, ее политического, правового, экономического и социального содержания с позиции общенациональной безопасности нашей страны.

2. **Введение:**

Дисциплина «Гуманитарные аспекты информационной безопасности», включенная в учебный план по основной образовательной программе бакалавриата по направлению 10.03.01 Информационная безопасность и специальности 10.05.02 Информационная безопасность телекоммуникационных систем, предоставляет возможности по эффективной и плодотворной гуманитаризации образования будущих технических специалистов, связанных с IT-сферой. Ее предназначение в учебном процессе можно определить так: расширить представление об информационной безопасности как о сфере, в которой задействованы не только технические устройства и люди, которые их обслуживают, но присутствует довольно обширная область, где происходит воздействие на волю и сознание человека и интенсивное информационно-коммуникационное взаимодействие различных социальных акторов. При этом в данном определении под взаимодействием предполагаются конфликтные отношения и интенции по оказанию деструктивного информационно-психологического эффекта в отношении противника (политического или геополитического соперника, или экономического конкурента и пр.).

Проблема обеспечения сохранности и целостности информации в тематических разделах курса «Гуманитарные аспекты информационной безопасности», таким образом, переводится из разряда чисто технической задачи по укреплению стабильности и защищенности информационной инфраструктуры (где человеческий фактор представлен лишь в виде прикладной задачи подготовки соответствующих компетентных специалистов, обслуживающих данную инфраструктуру) в рамки более широкого социокультурного контекста вопросов информационного взаимодействия и информационной безопасности. Данный контекст подразумевает антропологически фундированный мир, в котором субъектом и объектом информационных процессов выступает человек.

САМОСТОЯТЕЛЬНАЯ РАБОТА № 1 «Структура службы информационной безопасности»

Краткие теоретические сведения:

Общая структурная схема службы защиты информации

Управление КСЗИ должно осуществляться специализированной организационной структурой (системой управления информационной безопасностью - СУИБ), которая будет координировать действия подразделений (служб) организации, эксплуатирующей АС, контролировать реализацию политики безопасности информации и пресекать выявленные нарушения. Рассмотрим возможную структуру СУИБ без привязки к конкретной организационно-штатной структуре (Рис. 1. СУИБ). СУИБ строится как самостоятельная структура организации, подчиняющаяся непосредственно руководителю (заместителю руководителя) организации. В состав СУИБ обычно входит специализированное подразделение (отдел обеспечения безопасности информации, далее – отдел ОБИ), уполномоченные сотрудники подразделений и территориально разобщенных объектов, на которых распоряжением руководителя организации кроме основных задач дополнительно возложено решение задач по обеспечению безопасности информации (нештатные администраторы опасности, далее - администратор БИ); они управляют деятельностью (по вопросам обеспечения безопасности информации) и тесно взаимодействуют с администраторами АС (ее сегментов) и администраторами баз данных.

Примерная структура отдела ОБИ и основные взаимодействующие подразделения приведены на рис. 2. В состав отдела входят группы специалистов: главных и ведущих специалистов по защите информации, инженеров-программистов, отвечающих за отдельные направления в работе (за анализ состояния информационных баз, определение требований к защищенности различных подсистем АС и выбор методов и средств обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам обеспечения безопасности информации; за эффективное применение и администрирование штатных для операционных и систем управления базами данных и дополнительных специализированных средств защиты и анализа защищенности ресурсов автоматизированных систем). Отдел ОБИ является самостоятельным структурным подразделением организации и подчиняется заместителю руководителя организации, отвечающему за безопасность. Начальник отдела ОБИ назначается и освобождается от занимаемой должности по согласованию с руководителем организации.

Основные направления деятельности СУИБ

К основным направлениям деятельности СУИБ относится:

• выработка подходов к обеспечению безопасности информации и их практическая реализация, сбор статистических данных с целью анализа и выявления источников угроз и уязвимостей;

• составление и ведение схемы информационных потоков, проведение их анализа с целью выявления недостатков в организации КСЗИ, составление и выполнение планов по их устранению.

• координация усилий всех подразделений по вопросам обеспечения безопасности информации на предприятии;

• взаимодействие с подразделениями ОБИ организаций, учреждений, использующих информационные ресурсы;

• организация и выполнение технологических операций по предоставлению прав доступа сотрудникам к информационным ресурсам и средствам их обработки в соответствии с решениями, принятыми в установленном порядке;

• непосредственное обеспечение защиты информационных ресурсов, обрабатываемых с применением технических средств обработки, управление СЗИ;

• обеспечение защиты информации, циркулирующей в помещениях;

• доведение требований по обеспечению безопасности информации до сторонних организаций (партнеров), обращающихся к информационным ресурсам;

• проведение инструктажей сотрудников по мерам обеспечения безопасности информации, обучение их работе с использованием средств защиты информации;

• учет, хранение и выдача носителей информации, генерация паролей, ключей пользователей, используемых в СЗИ, контроль соответствия ПО АС эталонному;

• контроль правильности выполнения сотрудниками требований безопасности информации и расследование случаев их нарушения;

• оказание консультационной и технической поддержки пользователям АС при выполнении ими обязанностей по обеспечению безопасности информации;

• постановка и решение научно-технических задач и реализация технологических процедур вобласти обеспечения безопасности информации.

Для проведения соответствующих мероприятий по защите объекта должна быть создана специальная служба безопасности.

Задачи службы безопасности

Задачи службы безопасности крупного объекта заключаются в следующем:

1) определение основных направлений работы по обеспечению безопасности деятельности

объекта и его персонала, а также сохранности материальных ценностей и информации;

2) организация работы системы защиты объекта, разработка системы защиты на предпроектной стадии, участие в разработке технического проекта и его реализации, прикатил всех элементов системы защиты, поддержание системы защиты в работоспособном состоянии;

3) разработка нормативов работы с информацией всех категорий, контроль за соблюдением правил обработки, хранения и пересылки конфиденциальной информации;

4) разработка мер безопасности и правил обработки, хранения и транспортировки материальных ценностей и ценных бумаг, контроль за выполнением соответствующих нормативов;

5) организация обучения персонала объекта правилам соблюдения и поддержания режима безопасности деятельности объекта, проведение ежегодных квалификационных тестов;

6) организация и проведение (совместно с другими подразделениями объекта) мероприятий по защите;

7) взаимодействие с правоохранительными органами по вопросам безопасности персонала и имущества объекта.

Рис. 1 – Отдел информационной безопасности

Рис. 2 – Структуры службы безопасности

Задание:

1. Ответить на вопросы:

1) Для чего необходима служба информационной безопасности

2) Назовите основные должностные лица службы безопасности и их задачи

3) Каковы основные направления деятельности СУИБ

2. Сделайте структурную схему службы безопасности:

1) Больницы

2) Гостиницы

3) Администрации

4) Малого предприятия

5) Магазина

Пример:


СЛУЖБА БЕЗОПАСНОСТИ БАНКА
Отдел инженерной защиты
Отдел технических средств защиты
Отдел безопасности информации
Служба физической охраны
Группа работы с персоналом
здания, офисы, филиалы
обменные пункты
входы, лифты
сейфы, хранилища
охранная сигнализация
пожарная сигнализация
средства связи
авто-транспорт
инкассация
сертификация, лицензирование, защита информации
носители
оружие
детективные агентства
взаимодействие с правоохранительными органами
подбор
изучение
ЭВТ
бумажные
людские
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СЛУЖБА

САМОСТОЯТЕЛЬНАЯ РАБОТА № 2 “Функции основных групп службы безопасности”

Краткие теоретические сведения:

Группа режима

В ведении сотрудников этой службы находятся все вопросы, связанные с регламентацией деятельности персонала объекта и его посетителей.

Сотрудники группы режима

- определяют перечень сведений, составляющих коммерческую тайну, если таковые сведения не упомянуты в общегосударственных документах;
- разрабатывают положения и инструкции о порядке работы с конфиденциальной информацией и сведениями, составляющими тайну;
- организуют и ведут закрытое делопроизводство, учет пользования, хранение и размножение документов и других, носителей конфиденциальной информации;
- осуществляют допуск персонала объекта к работе с конфиденциальной информацией, разрабатывают и осуществляют проверки выполнения сотрудниками объекта регламента работы с такой информацией;
- участвуют в работе по повышению квалификации персонала, работающего с документами и другими носителями конфиденциальной информации;
- организуют и проводят изучение кандидатов для приема на работу, связанную с допуском к информации различных категорий конфиденциальности.

Группа охраны и сопровождения

Сотрудники этой группы обеспечивают физическую охрану объекта и его помещений с использованием соответствующих систем и средств, выявляют угрозы безопасности деятельности объекта, осуществляют защиту от угроз и их ликвидацию.

Кроме того, сотрудники этой группы участвуют

- в организации прохода персонала и посетителей в различные зоны безопасности;
- в наблюдении за обстановкой вокруг объекта и на его территории;
- в экстренных действиях при возникновении угроз чрезвычайных обстоятельств;
- в контроле работоспособности элементов системы защиты и их проверке;
- в мероприятиях по обеспечению безопасности транспортировки ценных грузов и документов.

При необходимости эта группа обеспечивает охрану отдельных лиц из числа персонала объекта

Техническая группа

Совместно с группой охраны сотрудники этой группы участвуют в обеспечении безопасности деятельности объекта с помощью технических средств защиты - систем сигнализации, наблюдения, связи и т.п. Сотрудники группы отвечают за бесперебойную работу всех технических средств системы защиты объекта, ремонтируют и настраивают аппаратуру защиты, готовят и реализуют предложения по повышению эффективности и совершенствованию технических средств защиты.

Кроме того, сотрудники этой группы выполняют задания

- по планированию и проведению мероприятий по специальной защите объекта и его помещений;

- по техническому обеспечению мероприятий детективной группы (а при необходимости участвуют в их проведении);

- по настройке и ремонту различных технических средств и оборудования, используемого в особо важных помещениях объекта;

- по выбору, заказу, приобретению и установке различных технических средств для службы безопасности объекта.

В связи с тем, что сотрудники технической службы должны иметь доступ в любые помещения объекта, необходимо особо тщательно отбирать и проверять кандидатов для работы в ее составе.

Детективная группа

Это специализированное подразделение разрабатывает и проводит специальные мероприятия по изучению отдельных лиц из числа персонала объекта, посетителей и клиентов фирмы и жителей ближайшего к объекту окружения, в действиях которых содержатся угрозы безопасности деятельности объекта. Кроме того, сотрудники детективной группы

- проверяют кандидатов для приема на работу на объекте;

- по отдельным заданиям руководства разрабатывают и проводят специальные мероприятия в отношении фирм-конкурентов;

- поддерживают контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта.

Для средних объектов (фирм) создаются группы безопасности, состоящие из сотрудников охраны и техников по настройке и ремонту средств защиты. Существует практика размещения разнообразных небольших предприятий и фирм в одном большом здании. Всеми вопросами безопасности в таких случаях занимается единая для всего здания служба безопасности, как правило, охраняющая помещения и персонал всех находящихся в здании фирм. Условно сотрудников службы информационной безопасности можно разделить по функциональным обязанностям:

Сотрудник группы безопасности. В его обязанности входит обеспечение контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в

своей зоне ответственности. При децентрализованном управлении каждая подсистема имеет своего сотрудника группы безопасности.

Администратор безопасности системы. В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (при необходимости) и за хранением резервных копий.

Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты набор данных, ужесточение защиты в случае необходимое, а также координирование работы с другими администраторами.

Руководитель группы. В его обязанности вход разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранное данных, оборудования и программного обеспечения, контроль за выполнением плана восстановления и последующее руководство административными группами в подсистемах ИС (при децентрализованном управлении)

В небольших организациях функции руководите службы обычно выполняет либо глава фирмы, либо его заместитель.

Количественный состав службы безопасности ограничен и зависит, прежде всего, от возможностей сам фирмы. Возможны различные варианты состава так группы. Кроме того, перечень необходимых знаний навыков, а также функциональных обязанностей, входящих в группу защиты информации может существенно отличаться в зависимости от назначения структуры и задач, решаемых в конкретной ИС.

Должностная инструкция инженера по защите информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая должностная инструкция определяет функциональные обязанности, права и ответственность Инженера по защите информации.

1.2. Инженер по защите информации назначается на должность и освобождается от должности в установленном действующим трудовым законодательством порядке приказом директора предприятия.

1.3. Инженер по защите информации подчиняется непосредственно.

1.4. На должность Инженера по защите информации назначается лицо, имеющее:

1.4.1. Требования к квалификации. Высшее профессиональное (техническое) образование без предъявления требований к стажу работы или среднее профессиональное (техническое) образование и стаж работы в должности техника по защите информации I категории не менее 3 лет либо других должностях, замещаемых специалистами со средним профессиональным образованием, не менее 5 лет.

1.5. Инженер по защите информации должен знать:

- постановления, распоряжения, приказы, методические и нормативные материалы по вопросам, связанным с обеспечением технической защиты информации; - специализацию предприятия и особенности его деятельности;

- методы и средства получения, обработки и передачи информации;

- научно-техническую и другую специальную литературу по техническому обеспечению защиты информации;

- технические средства защиты информации;

- программно-математические средства защиты информации;

- порядок оформления технической документации по защите информации;

- каналы возможной утечки информации;

- методы анализа и защиты информации;

- организацию работ по защите информации;

- инструкции по соблюдению режима проведения специальных работ;

- отечественный и зарубежный опыт в области технической разведки и защиты информации;

- основы экономики, организации производства, труда и управления;

- основы трудового законодательства;

- правила и нормы охраны труда.

2. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ

2.1. Функциональные обязанности Инженера по защите информации определены на основе и в объеме квалификационной характеристики по должности Инженера по защите информации и могут быть дополнены, уточнены при подготовке должностной инструкции исходя из конкретных обстоятельств.

2.2. Инженер по защите информации:

2.2.1. Выполняет работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и инженерно-технических мер защиты информационных систем, проводит исследования с целью нахождения и выбора наиболее целесообразных практических решений в пределах поставленной задачи.

2.2.2. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации.

2.2.3. Участвует в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации.

2.2.4. Составляет методики расчетов и программы экспериментальных исследований по технической защите информации, выполняет расчеты в соответствии с разработанными методиками и программами.

2.2.5. Проводит сопоставительный анализ данных исследований и испытаний, изучает возможные источники и каналы утечки информации.

2.2.6. Осуществляет разработку технического обеспечения системы защиты информации, техническое обслуживание средств защиты информации, принимает участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов.

2.2.7. Составляет информационные обзоры по технической защите информации. Выполняет оперативные задания, связанные с обеспечением контроля технических средств и механизмов системы защиты информации, участвует в проведении проверок учреждений, организаций и предприятий по выполнению требований нормативно-технической документации по защите информации, в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию.

2.2.8. Готовит предложения по заключению соглашений и договоров с другими учреждениями, организациями и предприятиями, предоставляющими услуги в области технических средств защиты информации, составляет заявки на необходимые материалы, оборудование, приборы.

2.2.9. Участвует в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

2.2.10. Проводит контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составляет и оформляет акты контрольных проверок, анализирует результаты проверок и разрабатывает предложения по совершенствованию и повышению эффективности принимаемых мер.

2.2.11. Изучает и обобщает опыт работы других учреждений, организаций и предприятий по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по ее защите и сохранению государственной тайны.

2.2.12. Выполняет работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ.

3. ОТВЕТСТВЕННОСТЬ

Инженер по защите информации несет ответственность за:

3.1. Невыполнение своих функциональных обязанностей.

3.2. Недостоверную информацию о состоянии выполнения полученных заданий и поручений, нарушение сроков их исполнения.

3.3. Невыполнение приказов, распоряжений директора предприятия, поручений и заданий начальника отдела.

3.4. Нарушение Правил внутреннего трудового распорядка, правил противопожарной безопасности и техники безопасности, установленных на предприятии.

4. УСЛОВИЯ РАБОТЫ

4.1. Режим работы Инженера по защите информации определяется в соответствии с Правилами внутреннего трудового распорядка, установленными на предприятии.

Задание:

Ответить на вопросы:

1) Перечислите основные групп службы безопасности
2) Перечислите задачи группы режима
3) Перечислите задачи группы охраны и сопровождения
4) Перечислите задачи технической группы
5) Перечислите задачи детективной группы

Опираясь на краткие теоретические сведения, составьте таблицу, ответив на следующие вопросы

1) Какими навыками должен инженер по защите информации
2) Функциональные обязанности инженера по защите информации
3) За что несет ответственность инженер по защите информации

САМОСТОЯТЕЛЬНАЯ РАБОТА № 3 “Цели и задачи службы информационной безопасности”

Краткие теоретические сведения:

Целями обеспечения безопасности предприятия являются:

- защита законных прав предприятия во взаимоотношениях с государственными органами, российскими и зарубежными партнерами и конкурентами; поддержание устойчивости порядка управления предприятием;

- сохранение собственности предприятия, ее рационального и эффективного использования в направлении удовлетворения общественных потребностей;

- повышение конкурентоспособности производимых товаров и услуг, создание благоприятной рыночной конъюнктуры для их реализации в условиях конкуренции на внутреннем и мировом рынке; рост прибылей предприятия;

- достижение внутренней и внешней организационной стабильности деятельности предприятия, надежности кооперированных связей и недопущение односторонней зависимости от случайных и недобросовестных партнеров;

- укрепление дисциплины труда и его производительности, формирование стимулов и условий повышения деловой активности сотрудников предприятия;

- максимально полное информационное обеспечение экономической, производственной и научно-технической деятельности предприятия, сохранение государственной и коммерческой тайны прав на интеллектуальную собственность, повышение эффективности использования имеющейся информации в мероприятиях по повышению деловой репутации предприятия среди российских и зарубежных партнеров.

К целям системы защиты информации предприятия также относится:

- предотвращение утечки, хищения, утраты, искажения, подделки информации: предотвращение угроз безопасности личности, предприятия, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокирования информации;

- предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;

- защита конституционных прав граждан на сохранение лично тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

- документированной информации в соответствии с законодательством.

Задачи и функции службы

Задачи обеспечения безопасности предприятия определяются необходимостью достижения названных целей и представляют собой требования на разработку и реализацию взаимосвязанных мер:

- своевременные выявления угроз жизненно важным интересам предприятия, причин и условий, благоприятствующих нанесению предприятию материального и морального ущерба, нарушению его нормальному функционированию и развитию, отработка механизма оперативного регулирования на угрозы и негативные тенденции в развитии;

- эффективного пресечения посягательств на законные интересы предприятия, использования юридических, экономических, организационных, социально-психологических, технических средств и средств массовой информации в выявлении и ослаблении источников угрозы его безопасности;

- максимально полного возмещения и локализации наносимого предприятию ущерба неправомерными действиями физических и юридических лиц, ослаблении негативного влияния последствий

- подрыва безопасности и неблагоприятных условий его деятельности на достижение стоящих перед предприятием целей;

- формирования надежных гарантий поддержания законности, взаимовыгодности, добросовестности сотрудничества предприятия, организационной стабильности его внешних и внутренних связей;

- обеспечения личной безопасности руководства, ведущих специалистов и лиц их семейств.

Основными задачами СБ являются:

1) обеспечение безопасности выполнения всех видов деятельности предприятия и сохранности информации и сведений, составляющих служебную и коммерческую тайну;

2) выявление и принятие мер, направленных на предотвращение возможности постороннего неправомерного вмешательства в деятельность структурных подразделений предприятия;

3) пресечение возможных каналов утечки информации и сведений, составляющих служебную и коммерческую тайну;

4) защита документов и переписки от фальсификации и подделок;

5) организация в зданиях предприятия (фирмы), включая склады, архивы и др., надежного пропускного и внутриобъектового режима и их охраны, внедрение имеющихся средств технического оснащения и охранной сигнализации;

6) обеспечение физической сохранности имущества предприятия, в том числе материальных носителей информации, содержащей коммерческие и иные секреты (документов, изделий, материалов, магнитных носителей и т.п.), а также секреты (документов, изделий, материалов, магнитных носителей и т.п.), а также личной безопасности персонала и клиентуры предприятия;

7) обеспечение режима безопасности при проведении всех видов деятельности, включая: встречи, переговоры, совещания, заседания и т.п. как на федеральном, так и на международном уровне;

8) предотвращение утечки информации, содержащей коммерческую тайну, в процессе производственной и иной деятельности предприятия, в том числе по техническим каналам утечки при использовании электронно-вычислительной техники и других технических средств;

9) организация учета, хранения и уничтожения документов, содержащих коммерческую тайну, а также постоянного контроля за соблюдением установленного порядка размножения документов, составляющих коммерческую тайну предприятия;

10) разработка и осуществление комплекса мероприятий по ограничению круга лиц, имеющих доступ к сведениям, составляющим коммерческую тайну предприятия;

11) получение совместно с другими подразделениями аналитическим и другим законным путем информации о конкурентах, клиентах и лицах из числа персонала, в действиях которых содержится угроза интересам предприятия, в частности, признаки возможной подготовки и осуществления неправомерных действий, связанных с недобросовестной конкуренцией, и подготовка предложений руководству по нейтрализации этих угроз;

12) оценка маркетинговых и ситуаций, и неправомерных действий ЗЛ и конкурентов;

13) разработка и проведение мероприятий по обеспечению защиты коммерческой тайны предприятия при осуществлении внешних связей (международных, научно технических, торгово-экономических и иных);

14) проведение воспитательно-профилактической работы с персоналом (а также его обучение) по вопросам обеспечения безопасности предприятия и защиты коммерческих секретов;

15) организация взаимодействия с правоохранительными организациями по вопросам безопасности персонала и имущества предприятия.

Задание:

Опираясь на краткие теоретические сведения, составьте таблицу, ответив на следующие вопросы

1) Кратко назовите основные цели службы информационной безопасности

2) Какие дополнительные цели выполняет служба информационной безопасности

3) Кратко назовите задачи службы информационной безопасности

САМОСТОЯТЕЛЬНАЯ РАБОТА № 4 “ Организационные основы и принципы деятельности службы информационной безопасности”

Краткие теоретические сведения:

Организация деятельности службы информационной безопасности

Деятельность Службы безопасности определяется ее целями и обеспечивает комплексное решение поставленных перед ней задач на основе стратегии и взаимосвязи тактических приемов подготовки и проведения мероприятий по обеспечению безопасности. СБ состоит из структурных единиц, осуществляющих разработку режимов безопасности, установление и поддержание этих режимов, а также контроль за их соблюдением. По решению Правления (дирекции) предприятия могут создаваться временные структуры с привлечением ведущих специалистов предприятия для решения сложных комплексных задач обеспечения безопасности, определяемых конкретными целями и складывающейся обстановкой. Для решения поставленных задач СБ предприятия в общем плане осуществляет:

- административно-распорядительную функцию, которая реализуется путем подготовки решений по установлению и поддержанию режимов безопасности, определению полномочий, прав, обязанностей и ответственности должностных лиц по вопросам обеспечения безопасности предприятия, а также по осуществлению представительских функций предприятия в данной области его деятельности;

- хозяйственно-распределительную функцию, которая реализуется путем участия СБ в определении ресурсов, необходимых для решения задач безопасности предприятия, в подготовке и проведении мероприятий по обеспечению сохранности имущества и интеллектуальной собственности предприятия, их рациональному использованию; учетно-контрольную функцию, которая реализуется выделением критически важных направлений финансово-коммерческой деятельности и организацией своевременного обнаружения угроз финансовой стабильности и устойчивости предприятия, оценкой их источников, налаживанием контроля за опасными ситуациями, ведением учета негативных факторов, влияющих на безопасность предприятия, а также накоплением информации о недобросовестных конкурентах, ненадежных партнерах, лицах и организациях, посягающих на жизненно важные интересы государственного предприятия;

- социально-кадровую функцию, которая реализуется участием СБ в расстановке кадров, выявлении негативных тенденций в трудовых коллективах, возможных причин и условий социальной напряженности, в предупреждении и локализации конфликтов, инструктаже работников предприятия по вопросам безопасности, формировании у них чувства ответственности за соблюдение установленных режимов безопасности. СБ

участвует в решении вопросов, связанных с командированием в установленном порядке специалистов предприятия за границу.

- организационно-управленческую функцию, которая реализуется путем оказания управленческого воздействия на создание, поддержание и своевременную реорганизацию постоянной организационной структуры и управления процессом обеспечения безопасности предприятия, гибких временных структур по отдельным направлениям работы, организации взаимодействия и координации между их отдельными звеньями для достижения заданных программных целей;

- планово-производственную функцию, которая реализуется разработкой комплексной программы и отдельных целевых планов обеспечения безопасности предприятия, подготовкой и проведением мероприятий по их осуществлению, установлению и поддержанию режимов безопасности;

- организационно-техническую функцию, которая реализуется путем материально-технического и технологического обеспечения режимов безопасности на предприятии, освоением специальной техники и достижений соответствующего потребностям обеспечения безопасного уровня, содействием в освоении новых прогрессивных видов техники и технологий режимно-секретной и другой специальной деятельности; научно методическую функцию, которая реализуется путем накопления и распространения передового опыта обеспечения безопасности предприятия, организацией обучения его штатного контингента, научной разработки возникающих перед предприятием проблем обеспечения безопасности и методического сопровождения его деятельности в этой сфере;

- информационно-аналитическую функцию, которая реализуется путем целенаправленного сбора, накопления и обработки информации, относящейся к сфере безопасности, создания и использования необходимых для этого технических и методических средств аналитической обработки информации, организации информационного обеспечения заинтересованных подразделений и отдельных лиц предприятия в сведениях, имеющихся в СБ.

Принципы организации службы

Принципы организации СБ выражают основополагающие требования к стратегии и тактике, организации и осуществлению мероприятий по защите жизненно важных интересов предприятия, концентрируют опыт успешного решения задач в этой сфере деятельности.

- Законность. Меры безопасности предприятия разрабатываются на основе норм права в пределах определенной данным типовым положением компетенции с применением всех дозволенных Законом методов обнаружения и пресечения правонарушений в сфере безопасности.

- Самостоятельность и ответственность. СБ располагают всеми необходимыми для своей деятельности видами ресурсов, при использовании

которых обеспечивается строгое соответствие производимых затрат и достигаемых результатов, материальная ответственность инициаторов и исполнителей соответствующих мероприятий за результаты своей деятельности.

- Экономическая целесообразность и прибыльность. Мероприятия по обеспечению безопасности предприятия не должны приводить к ухудшению экономических показателей деятельности предприятия, а стабильность его прибылей является главным критерием оценки качества работы СБ, определения размеров материального вознаграждения их сотрудников.

- Специализация и профессионализм. Кадровый состав подразделений безопасности специализируются по направлениям комплексного обеспечения безопасности предприятия. Профессиональная подготовка сотрудников СБ предприятия должна позволять широко использовать научные достижения и передовой опыт организации работ обеспечению безопасности объектов. В противном случае противодействия ЗЛ становятся проблематичными.

- Программно-целевое планирование. Деятельность СБ предприятия по обеспечению безопасности осуществляется на основании комплексной программы и разрабатываемых на ее основе планов работ и отдельных мероприятий.

- Взаимодействие и координация. Меры безопасности осуществляются на основе взаимодействия скоординированности усилий всех заинтересованных подразделений предприятия, а также установления необходимых связей с внешними организациями (органами государственного управления, правоохранительными органами, другими предприятиями и фирмами). Деятельность в сфере безопасности не должна нарушать нормальных условий работы предприятия на других направлениях.

- Гласность в сочетании с необходимой конспирацией. Руководящие органы предприятия регулярно «формируют своих сотрудников о мероприятиях по обеспечению безопасности. В оправданных ситуациях меры безопасности могут носить конспиративный характер. Конспиративность мер безопасности предполагает специальную организацию контроля руководящих органов СБ предприятия за их применением, соблюдением необходимых правил- процедур.

Задания:

1. Ответить на вопросы:

1) Чем определяется деятельность СБ
2) Расскажите про хозяйственно-распределительную функцию
3) Расскажите про организационно-техническую функцию
4) Расскажите про информационно-аналитическую функцию
5) Расскажите про планово-производственную функцию
6) Расскажите про социально-кадровую функцию
7) Назовите основные принципы организации службы безопасности

2. Тестирование:

1. Следующее структурное подразделение службы защиты информации отвечает за

контакты с правоохранительными органами по всем вопросам обеспечения

безопасности деятельности объекта

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

2. В обязанности какого сотрудника входит разработка и поддержка эффективных

мер защиты по обработке информации для обеспечения сохранное данных

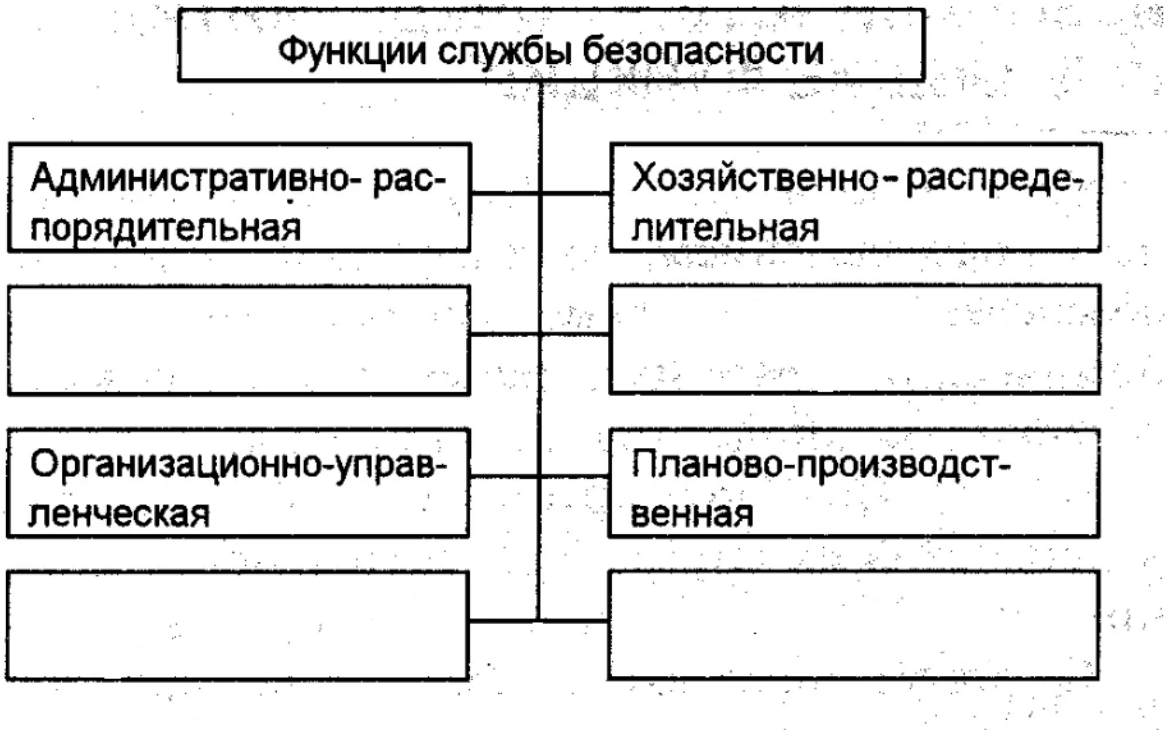
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

3. В обязанности какого сотрудника входит контроль за выполнением плана

восстановления после инцидента информационной безопасности

- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

3. Дополните схему:


Функции службы безопасности
Административно- распорядительная
Хозяйственно - распределительная
Организационно-управленческая
Планово-производственная

САМОСТОЯТЕЛЬНАЯ РАБОТА № 5 “Лицензирование видов деятельности службы безопасности”

Краткие теоретические сведения:

Лицензирование видов деятельности службы безопасности предприятия

В соответствии с Федеральным законом «О лицензировании отдельных видов деятельности» от 8.08.2001 года №128-ФЗ деятельность различных подразделений службы безопасности предприятия подпадает под требования этого закона, по которому подлежит лицензированию (при наличии этих видов деятельности): предоставление услуг в области шифрования информации;

деятельность:

1. по выявлению электронных устройств, предназначенных для негласного получения информации;
2. разработке и производству средств защиты конфиденциальной информации;
3. технической защите конфиденциальной информации;
4. предупреждению и тушению пожаров;
5. разработка, производство и приобретение с целью продажи спецсредств для негласного получения информации;

негосударственная (частная) охранная и сыскная деятельность.

Под лицензией понимается специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому или физическому лицу.

Лицензирование - процесс, связанный с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензии, приостановлением, возобновлением или контролем лицензирующих органов за соблюдением правил выполнения лицензионных видов деятельности.

Срок действия лицензии не может быть менее чем 5 лет, в отдельных случаях предусматривается бессрочное действие лицензии.

Существует определенный порядок принятия решения о предоставлении лицензии, которая может быть выдана лицензирующим органом на основании следующих документов:

- заявление о предоставлении лицензии;
- копии учредительных документов и копии свидетельства о госрегистрации;
- копии свидетельства о постановке на учет в налоговом органе;
- документ, подтверждающий уплату лицензионного сбора.

Дополнительные условия и правила лицензирования существуют при получении разрешений определенных видов деятельности в области защиты информации (решение Гостехкомиссии и ФАПСИ от 27.04.94г. №10) и деятельности по технической защите конфиденциальной информации (Постановление Правительства РФ 30.04.02г. №290). Эту систему лицензирования организуют государственные органы по лицензированию, которыми являются Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России) и Федеральное агентство правительственной связи и информации при Президенте Российской'Федерации (ФАПСИ). Государственные органы по лицензированию в пределах их компетенции, установленной законодательством Российской Федерации, осуществляют лицензирование деятельности предприятия в области защиты информации в соответствии с существующими перечнями видов деятельности. Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию Гостехкомиссией России:

• Сертификация, сертификационные испытания защищенных технических средств обработки информации (ТСОИ), технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств по требованиям безопасности, программных средств защиты информации, программных средств контроля защищенности информации.

• Аттестация систем информатизации, автоматизированных систем управления, систем связи и передачи данных, технических средств приема, передачи и обработки подлежащей защите информации, технических средств и систем, не обрабатывающих эту информацию, но размещенных в помещениях, где она обрабатывается (циркулирует), а также помещений, предназначенных для ведения переговоров, содержащих охраняемые сведения, на соответствие требованиям руководящих и нормативных документов по безопасности информации и контроль защищенности информации в этих системах, технических средствах и помещениях.

• Разработка, производство, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание защищенных ТСОИ, технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств защиты информации, программных средств контроля защищенности информации.

• Проектирование объектов в защищенном исполнении.

• Подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне. Перечень видов

деятельности предприятий в области защиты информации, подлежащих лицензированию ФАПСИ

• Разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка и ремонт шифровальных средств, предназначенных для криптографической защиты информации при ее обработке, хранении и передаче по каналам связи, а также предоставление услуг по шифрованию информации.

• Эксплуатация государственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

• Разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание специализированных защищенных ТСОИ, технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств защиты информации, программных средств контроля защищенности информации, предназначенных для использования в высших органах.

• Подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне. Лицензия на право деятельности по защите информации (далее - лицензия) выдается предприятию государственным органом по лицензированию по представлению органа государственной власти Российской Федерации на конкретные виды деятельности на три года, по истечении которых осуществляется ее перерегистрация в порядке, установленном для выдачи I/ лицензии. Лицензия выдается подавшему заявку на ее получение предприятию-заявителю, располагающему производственной и испытательной базой, нормативной и методической документацией, научным и инженерно-техническим персоналом, при условии их соответствия требованиям государственного органа по лицензированию на основании результатов экспертизы деятельности предприятия по заявленному направлению работ. С этими требованиями заявитель имеет право ознакомиться в государственном органе по лицензированию.

Для получения лицензии в этом случае представляется расширенный комплект документов: заявление; представление органа государственной власти Российской Федерации; материалы экспертизы, подтверждающие наличие необходимых условий для проведения работ по заявленным видам деятельности, а также профессиональную пригодность руководителя предприятия-заявителя или лиц, уполномоченных им для руководства лицензируемой деятельностью; копии документов о государственной регистрации предпринимательской деятельности и устава предприятия.

Отказ в выдаче лицензии производится в случаях, если отсутствуют необходимые условия для проведения работ по заявленному виду деятельности; профессиональная подготовка руководителя предприятия-заявителя, или лиц, уполномоченных им для руководства лицензируемой деятельностью, не соответствует установленным требованиям; в представленных для получения лицензии документах указаны недостоверные сведения; заявитель в установленном законом порядке признан виновным в недобросовестной конкуренции в лицензируемой деятельности.

Задание:

Пройдите тест

1) Выберите стороны, участвующие в процессе лицензирования:

1) Юридическое лицо и ФСТЭК России

2) Орган по аттестации и испытательная лаборатория

3) Заявитель и орган по аттестации

4) Заявитель и юридическое лицо

5) Физическое лицо и орган по сертификации

2) Какую лицензию должна получить испытательная лаборатория для проведения работ по сертификации средств защиты информации, используемых на объектах информатизации, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну?

1) На проведение работ, связанных с созданием средств защиты информации

2) На осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну

3) На деятельность по технической защите конфиденциальной информации

4) На деятельность по разработке и производству средств защиты конфиденциальной информации

3) Какую лицензию должен получить орган по аттестации для проведения работ по аттестации объектов информатизации?

1) На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации)

2) На деятельность по технической защите конфиденциальной информации.

3) На проведение работ, связанных с созданием средств защиты информации.

4) На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны

4) Чем определены сроки и последовательность прохождения процедур для получения лицензии на деятельность по разработке и производству средств защиты конфиденциальной информации?

1) Федеральным законом
2) Постановлением Правительства
3) Руководящим документом
4) Административным регламентом
5) Нормативным документом
6) Положением
7) ГОСТом
8) Рекомендациями по стандартизации

5) Государственная система защиты информации включает в себя:

1) Подсистему сертификации СЗИ и подсистему лицензирования в области ЗИ
2) Подсистему сертификации СЗИ и подсистему аттестации ОИ
3) Подсистему лицензирования в области ЗИ и подсистему аттестации ОИ
4) Подсистемы лицензирования деятельности предприятий в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизации

6) Выберите объект испытаний при проведении процедуры лицензирования:

1) Объект информатизации
2) Средство защиты информации
3) Автоматизированная система
4) Юридическое лицо

7) Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности это:

1) Аттестат аккредитации
2) Сертификат соответствия
3) Лицензия
4) Аттестат соответствия
5) Заключение
6) Предписание

8) Какую лицензию должна получить испытательная лаборатория для проведения работ по сертификации средств защиты информации, используемых на объектах информатизации, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну?

1) На проведение работ, связанных с созданием средств защиты информации

2) На осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну

3) На деятельность по технической защите конфиденциальной информации

4) На деятельность по разработке и производству средств защиты конфиденциальной информации

9) Чем определены сроки и последовательность прохождения процедур для получения лицензии на деятельность по разработке и производству средств защиты конфиденциальной информации?

1) Федеральным законом
2) Постановлением Правительства
3) Руководящим документом
4) Административным регламентом
5) Нормативным документом
6) Положением
7) ГОСТом
8) Рекомендациями по стандартизации

САМОСТОЯТЕЛЬНАЯ РАБОТА № 6 “Управление службой защиты информации”

Краткие теоретические сведения:

Методы управления СБП

Основной целью деятельности СБП является своевременное пересечение (нейтрализация) противоправных посягательств на экономические интересы, персонал предприятия, предотвращение материального и физического вреда, а также предотвращение и пресечение преступлений, административных проступков и гражданско- правовых конфликтов и т.д.

Формулирование цели управления зависит от многих факторов: финансовых возможностей предприятия-учредителя, его географического месторасположения, возможности набрать из числа жителей данной территории квалифицированный состав сотрудников службы безопасности и т.д.

На основе сформулированной цели проектируется и создается оргструктура службы безопасности. Анализ изученных документов службы безопасности свидетельствует, что наибольшее распространение получили линейная и линейно-штабная структура. Линейная структура характеризуется четким единоначалием - каждый сотрудник подчинен только одному вышестоящему лицу.

Линейно-штабная структура представляет собой линейную структуру, дополненную штабным органом (штабом), на который возлагаются дополнительные функции управления. Такая структура создается обычно тогда, когда большое количество сотрудников или их территориальная разобщенность не позволяют начальнику службы безопасности эффективно управлять.

Эффективное функционирование службы безопасности предполагает предварительную проработку многих вопросов. Среди них особое значение приобретает проектирование оргструктуры службы безопасности и ее ресурсного обеспечения, т.к. без решения этих вопросов ее деятельность вообще невозможна. Собственно говоря, употребляемый нами многозначный термин «организация» среди многих значений имеет и такое, как создание нужной структуры и необходимых ресурсов.

Общеизвестно, что любое оргструктурное формирование создается для реализации определенных функций. Применительно к службе безопасности предприятия эти функции определены ст. 3 закона РФ «О частной детективной и охранной деятельности в Российской Федерации». Этим законом (ст.14) предусмотрена должность руководителя службы безопасности, которая на практике реализуется в виде начальника службы безопасности (здесь сказался прошлый опыт деятельности в правоохранительных органах персонала

службы безопасности). Совершенно очевидно, что, если персонал службы безопасности по количеству большой, неизбежно встает вопрос о заместителях начальника службы безопасности. Их может быть несколько (обычно по количеству подразделений службы безопасности). Как правило, заместитель начальника службы безопасности является одновременно руководителем одного из подразделения и, в свою очередь, также имеет одного или нескольких заместителей. Не вызывает сомнений целесообразность создания таких подразделений, как канцелярия и бухгалтерия (в случае, если службу безопасности не обслуживает единая бухгалтерия предприятия-учредителя).

В крупных службах безопасности, где возникает необходимость создания штабных подразделений, так как начальники службы безопасности просто физически не способны на должном уровне выполнять такие управленческие функции, как анализ, планирование, контроль и т.д., исполнение этих обязанностей помощниками положение дел не меняет, так как в этом случае возникает необходимость их повседневного руководства, что опять-таки не под силу начальнику службы безопасности, и он вынужден будет назначить одного из них координатором деятельности других, а это, по сути, означает выполнение обязанностей начальника штаба. Предложенная схема оргструктуры может время от времени уточняться и пересматриваться. Любая оргструктура, даже самая оптимальная, не сможет дать ожидаемых результатов, если ее не дополнить внутренними нормативными актами, регулирующими деятельность всех подразделений и сотрудников службы безопасности. Образно выражаясь, «кость» (оргструктура) должна обрасти «мясом» (нормативными документами). Причем эти нормативные акты условно можно разделить на две группы: непосредственно относящиеся к деятельности самой службы безопасности и к деятельности других служб (подразделений, сотрудников) предприятия. Методы управления службой безопасности подразделяются на три группы:

экономические;

организационно-распорядительные;

социально-психологические.

Руководители службы безопасности должны безупречно владеть всеми методами управления в их единстве. Для этого они должны знать особенности каждого из них.

Экономические методы управления строятся на использовании различных экономических стимулов, таких, например, как заработная плата. Умелое использование этого стимула с учетом уровня профессионализма, стажа работы, результатов деятельности сотрудника и т.д. позволяет эффективно организовать работу отдельных сотрудников в рамках службы безопасности.

Организационно-распорядительные методы управления (приказы, распоряжения, указания, инструкции и т.д.) подразделяются на три группы:

распорядительные,

организационно-стабилизирующие

дисциплинирующие

Особое внимание в деятельности службы безопасности следует уделить таким нормативам (производные от организационно- стабилизирующих методов) как нормативы времени выполнения той или иной деятельности, численности сотрудников того или иного подразделения и т.д. Такие нормативы обычно перенимаются из опыта работы органов внутренних дел, ФСБ и т.д., с поправкой на специфику деятельности службы безопасности предприятия, фирмы.

Социально-психологические методы основаны на использовании моральных стимулов к труду и воздействуют на личность сотрудника службы безопасности с помощью психологических приемов с целью превращения задания в осознанный долг, внутреннюю потребность человека. Это достигается посредством приемов, которые носят личностный характер (личный пример, авторитет и т.д.). На уровне коллектива службы безопасности действуют методы, включающие оценку индивидуальных качеств сотрудников и выработку ориентиров, создающих условия для максимального проявления их профессиональных качеств.

Структура процесса управления в самом общем виде состоит из трех стадий, каждая из которых включает в себя последовательно осуществляемые этапы или операции:

1. Сбор, обработка, обобщение и анализ информации

2. Выработка и принятие управленческого решения.

3. Организация исполнения управленческого решения.

При разработке управленческих подходов для решения конкретных вопросов по предотвращению различных угроз необходимо учитывать различные режимы функционирования СПБ: повседневной деятельности, повышенной готовности и при чрезвычайном положении (кризисной ситуации).

Функции процессов управления

При рассмотрении основных процессов управления выделяют следующие типовые функции:

- Прогнозирование
- Планирование
- Организация
- Регулирование
- Мотивация
- Контроль

В системе управления все эти функции должны быть объединены в целостный процесс, хотя из методических соображений целесообразно рассматривать их отдельно. Рассмотрим далее указанные функции с учетом специфики деятельности службы безопасности. Прогнозирование предполагает составление заключения (прогноза) о будущих событиях и тенденциях развития службы безопасности. Прогнозные оценки бывают оперативными (с упреждением не более одного месяца), краткосрочными (от 1 месяца до 1 года), среднесрочными (от 1 года до 5 лет). Составляются они как привлеченными со стороны специалистами, так и сотрудниками службы безопасности (в первую очередь сотрудниками штаба). Качество прогнозных оценок повышается, если они составляются сотрудниками службы безопасности с помощью приглашенных экспертов - специалистов в той или иной области. Представляется, что наиболее целесообразным было бы составление следующих видов прогнозных оценок: криминологических; рисковых (коммерческий, финансовый и т.д.) в предпринимательской деятельности; экономических, физических, информационных и т.д., определяющих безопасность предприятия.

Принципы управления СБП

Принципы управления службой безопасности определяют требования к системе структуре и организации процесса управления. В рамках службы безопасности — это следующие принципы:

1. Научность. Основное содержание этого принципа заключается в требовании, чтобы все управленческие действия осуществлялись на базе применения научных методов и подходов, Между прочим, этот принцип требует от руководителей службы безопасности и его подразделений внимательного изучений управленческой и специальной литературы по проблемам обеспечения! безопасности предприятия.

2. Единоначалие и коллегиальность. Сущность этого принципа заключается в том, что на основе мнений низовых руководителей и рядовых исполнителей конкретных решений, вышестоящий начальник пользуется правом единоличного решения вопросов, входящих в его компетенцию.

3. Принцип системности и комплексности. Системность означает необходимость использования элементов теории больших систем, системного анализа в каждом управленческом решении. Комплексность в управлении означает необходимость всестороннего охвата управляемой системы, учета всех сторон, всех направлений, всех свойств. Этот принцип требует от руководителей службы безопасности выработки у себя аналитико-синтетического склада мышления.

4. Принцип оптимального сочетания централизации и децентрализации. Этот принцип состоит в оптимальном распределении (делегировании) полномочий при принятии управленческих решений. Здесь следует руководствоваться таким правилом: тот, кому предстоит выполнять

управленческое решение, должен его самостоятельно разработать и, с учетом возможных коррективов вышестоящего руководства, активно добиваться его реализации.

5. Принцип плановости. Сущность этого принципа состоит 1 установлении основных направлений и пропорций службы безопасности1 в перспективе. Практическая реализация этого принципа означает, что все сотрудники, подразделения и службы безопасности в целом должны планировать свою деятельность в такой последовательности: служба безопасности – подразделения – сотрудник.

6. Принцип сочетания прав, обязанностей ответственности. Этот принцип предполагает, что каждый сотрудник службы безопасности должен выполнять возложенные на него обязанности, при этом он наделяется адекватными ему правами и несет ответственность за качество их выполнения.

Обеспечение деятельности службы безопасности

Для успешного функционирования и эффективного управления службой безопасности необходимо обеспечить ее материально-техническими, финансовыми, кадровыми и информационными ресурсами.

Среди них первостепенное значение имеют финансовые ресурсы. Без финансового обеспечения деятельности службы безопасности бессмысленно вообще говорить о ее функционировании.

Поскольку служба безопасности не вправе самостоятельно зарабатывать деньги путем заключения договоров с другими клиентами, именно на предприятии-учредителе лежит обязанность финансирования ее деятельности. Но это не означает, что руководство службы безопасности должно занимать в этом вопросе пассивную позицию. Напротив, обоснованные текущие и прогнозные оценки в финансовых потребностях службы безопасности и основанные на них точные расчеты должны стать правилом, а не исключением. Финансовую политику службы безопасности определяют, конечно, ее руководители, но при этом активную помощь им должна оказывать бухгалтерская служба.

В функции этой службы входит ведение табеля, учета рабочего времени; начисление зарплаты, премий и т.д.; учет выплат за различные услуги; перечисление денег; выдача сотрудникам их денежного содержания; оплата счетов и т.д. Поскольку руководители службы безопасности не являются, как правило, специалистами в финансовых вопросах, наиболее целесообразно свое внимание сосредоточить им на некоторых ключевых моментах.

Во-первых, периодически проверять финансовое состояние службы безопасности с помощью приглашенных специалистов. Во-вторых, открывать расчетные и текущие счета только в надежных банках. В-третьих, добиваться такого уровня минимальной зарплаты персонала службы безопасности, чтобы у него не возникало соблазна увольняться (можно порекомендовать я связи с

этим устанавливать в контрактах сумму зарплаты в иностранной валюте по курсу Центрального банка России на день его выдачи). В-четвертых, установить поэтапное финансирование закупленных (приобретенных) материально-технических средств от наиболее необходимых (например, в первую очередь, оружие, спецсредства) до менее необходимых (например, канцелярские принадлежности и т.д.). Наконец, рационально и обоснованно использовать деньги из фонда поощрения и материальной помощи персоналу.

Полное и качественное обеспечение деятельности службы безопасности материально-техническими ресурсами – не только средство, но и условие повышения эффективности работы его сотрудников Эти ресурсы условно подразделяются на следующие группы:

· оружие и боеприпасы;

· специальные средства;

· служебные помещения различного характера (кабинеты, караульные помещения, оружейные комнаты, стрелковые тиры, комнаты досмотра);

· вспомогательная техника (автотранспорт, видео, кино, фототехника, средства оперативной радио- и телефонной связи, компьютеры и т.д.);

· средства предупреждения и защиты (охранно-пожарная сигнализация, сторожевые собаки, охранное освещение, телевидение т.д.);

· средства обеспечения нормальной деятельности сотрудников (форменное обмундирование, мебель, канцелярские принадлежности, медикаменты, бланки документов, юридическая и специальная литература и т.д.).

Обеспечение оружием, боеприпасами, спецсредствами сотрудников службы безопасности регламентировано законом информативными актами правительства, МВД и Министерстве финансов России. В отношении обеспечения некоторых средств целесообразно использовать нормативы, имеющиеся в различных министерствах и ведомствах (количество служебных собак, оборудование и размеры стрелкового тира, наличие медикаментов, расчет различных видов охранно-пожарной сигнализации и т.д.).

Наконец, последнее по счету, но не по важности, обеспечение деятельности службы безопасности информационными ресурсами.

Прежде всего, следует определить потребность и объемы минимума информации, без которых функционирование службы безопасности вообще невозможно. Такую информацию можно условно разделить на три блока («Среда функционирования предприятия», «Состояние безопасности внутри предприятия» и «Внутриорганизационная деятельность службы безопасности»), после чего в рамках каждого блока разработать перечень необходимых сведений. Этот перечень не будет носить произвольный характер, если при его составлении руководствоваться одним принципом: любая информация реально должна «обслуживать», «работать» на реализацию, как минимум, одной функции службы безопасности. Можно

рекомендовать в этой связи включать в указанные блоки следующие сведения, которые, разумеется, не могут быть исчерпывающими.

В 1-й блок «Среда функционирования предприятия» возможно включение сведений о предприятиях-конкурентах, правоохранительных и контрольно-надзорных органах, рыночной конъюнктуре, криминогенной ситуации в районе месторасположения предприятия, нормативных актах, регулирующих деятельность предприятия-учредителя и т.д.

Во 2-й блок «Состояние безопасности внутри предприятия» целесообразно включить следующие сведения: состояние преступности среди персонала, наличие или отсутствие коммерческой тайны, источники (каналы) и суммы материального ущерба, наносимого предприятию, анализ насильственных преступлений, совершенных против его персонала, эффективность работы юрисконсульта (юридической службы), о сотрудниках предприятия, имеющих доступ к конфиденциальной информации, с корыстно-насильственной мотивацией, связанных с сохранностью товарно-материальных ценностей; местонахождении и правилах работы с документацией, содержащей коммерческую тайну; месторасположении и состоянии сохранности изделий (описания процесса), составляющих секрет предприятия и т.д.

Наконец, в 3-м блоке «Внутриорганизационная деятельность службы безопасности» желательно иметь сведения о составе и структуре службы безопасности, перемещениях сотрудников, дисциплинарной практике, результатах проверок, состоянии законности» и т.д.

Совершенно очевидно, что без надлежащей организации такого: массива информации, удобной и практичной для использования, не обойтись. Идеальным вариантом в этом случае было бы создание информационной системы на базе компьютерной техники, однако его создание требует определенных финансовых затрат. Поэтому на практике чаще всего встречается отражение и систематизация необходимой информации в письменных документах. К документам, составляемым в службе безопасности, относятся:

- организационные документы (устав, положение, должностные инструкции, штатное расписание, правила внутреннего трудового распорядка);
- правовые документы (законы, подзаконные акты, методические рекомендации по проблемам безопасности и т.д.);
- распорядительные документы (приказы, инструкции, указания, графики работы персонала и т.д.);
- информационно-справочные документы (протоколы, акты, справки, письма, докладные и объяснительные записки, телефонограммы, телеграммы, досье и т.д.);
- договоры, трудовые соглашения;

- документы по личному составу (приказы по личному составу, трудовые книжки, материалы проверок по жалобам, графики отпусков и т.д.).

В результате правильно организованного документального отражения необходимых сведений достигается эффективное информационное обеспечение деятельности службы безопасности.

Управление безопасностью предприятия в кризисных ситуациях

Служба безопасности должна быть всегда готова к возникновению критических (кризисных) ситуаций, проявляющихся в результате столкновения интересов бизнеса и преступного мира.

Кризисная ситуация – это проявление фактов угроз со стороны отдельных лиц или групп. Кризисная ситуация может проявляться и развиваться по-разному: медленно или спонтанно, мгновенно.

При оценке и анализе кризисной ситуации очень важно, как можно быстрее определиться с ответом на вопрос, способна ли СБП справиться с ситуацией своими силами либо для ее разрешения необходимо привлечение правоохранительных органов. Однако в любом случае, учитывая возможность возникновения кризисных ситуаций, любая фирма стремится создать в составе СБП отдельное формирование, именуемое КРИЗИСНАЯ ГРУППА. Она создается из числа ключевых фигур фирмы: директор, руководители линейных подразделений, филиалов, служб, юрист, главный бухгалтер и др. Кризисная группа может быть создана на постоянной основе с непременным включением в число ее членов: руководителя фирмы, юриста, финансиста, руководителя службы безопасности.

Руководство кризисной группой может быть возложено на главу фирмы. Перечисленные лица, как правило, в силу своего служебного положения, обладания специальными знаниями, опытом располагают реальными возможностями достаточно эффективно воздействовать на обстоятельства, в условиях которых возникает и протекает кризисная ситуация, не выпуская при этом рычагов влияния на повседневную коммерческую и производственную деятельность.

В каждом конкретном случае в состав кризисной группы могут включаться и иные специалисты.

Кризисная группа решает следующие задачи:

· оценка обстановки;

· принятие неотложных мер по безопасности;

· управление деятельностью фирмы в экстренных условиях;

· обеспечение оперативного взаимодействия с органами правопорядка.

Главная цель создания кризисной группы – противодействие внешним угрозам безопасности фирмы. Рабочие заседания группы должны проходить в условиях предельной конфиденциальности.

Как правило, деятельность кризисной группы регламентируется типовым планом действий руководства и персонала фирмы. В зависимости от складывающейся ситуации планы могут быть следующего вида, а именно, план действий: при угрозе взрыва, захвате заложников или похищении сотрудников фирмы, вымогательстве, нападении на помещения фирмы, нападении на инкассаторов.

Типовые кризисные планы являются документами конфиденциального характера, доступ к которым должен иметь узкий круг лиц. Составляться подобные планы должны не более чем в двух-трех экземплярах. Один хранится у руководителя, другой – у начальника службы безопасности, третий может находиться у лица, замещающего руководителя фирмы в его отсутствие.

Осуществляя планирование, надо исходить из того, что план – это не набор мероприятий, а последовательная линия поведения, стратегия деятельности фирмы в конкретной кризисной ситуации, направленная на обеспечение эффективной безопасности.

Роль персонала в системе защиты информации:

Системы защиты и охраны проектируют, строят и используют люди, обслуживают технику и технологический процесс любого предприятия также люди. Они должны быть надежны.

Обеспечение надежности персонала службы защиты информации - это совокупность мер, включающих в себя анализ и оценку степени честности и благонадежности сотрудников с целью гарантировать защиту информации, обеспечить ее целостность и конфиденциальность.

К мерам по обеспечению надежности персонала относятся:

· выполнение обязательств сотрудниками в том, что они будут обеспечивать защиту и тайну информации, к которой они имеют доступ в силу своих профессиональных обязанностей;

· создание благоприятного производственного климата для всех сотрудников службы безопасности.

Специалисты по защите информации приводят данные, утверждающие, что определяющей фигурой в обеспечении сохранности ценных сведений предприятия является его сотрудник.

Угроза, исходящая от некомпетентности служащих, по мнению экспертов, основывается на алгоритмической уязвимости информационных систем, которая не исключает возможности некомпетентных действий и может привести к сбоям системы.

Неудовлетворенные служащие также предоставляют внутреннюю угрозу. Они опасны тем, что имеют легальный доступ. То же можно сказать и про нечестных служащих.

В связи с этим представляется целесообразным с целью обеспечения информационной безопасности коммерческих структур уделять большее

внимание подбору и изучению кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи.

Следует особо подчеркнуть, что наиболее неуправляемым элементом в системе защиты информации является персонал. Правильная кадровая политика и организация управления персоналом позволяют снизить риски этого фактора. Задача обеспечения информационной безопасности должна решаться на всех уровнях управления предприятием. Рассмотрим их более подробно в трех направлениях.

Безопасность при выборе персонала и работе с ним:

Необходимо включить задачи по обеспечению безопасности в должностные обязанности всех сотрудников.

При приеме на работу рекомендуется проводить проверку рекомендаций, данных из резюме, подтверждение ученых степеней и образования, идентификацию личности, проверку на полиграфе при добровольном согласии кандидата на должность, включение соглашения о соблюдении режима информационной безопасности в условия трудового договора с работником.

При приеме на работу новых сотрудников необходимо, чтобы они ознакомились и подписали письменную формулировку их должностных обязанностей и прав доступа к ресурсам компании (в том числе и информационным), соглашение о конфиденциальности, специальные соглашения об ознакомлении со всеми видами служебной корреспонденции (мониторинг сетевых данных, телефонных переговоров, факсов и т.д.).

Подготовка и переподготовка пользователей и специалистов по защите информации:

Необходимы регулярное проведение тренингов для персонала и контроль готовности новых сотрудников по применению правил информационной защиты, а также периодическая переподготовка специалистов подразделений защиты информации. Особенно важно проводить тренинги при изменении конфигурации информационной системы.

Задание:

1. Ответить на вопросы:

1) На какие группы подразделяются методы управления службой безопасности и их краткое описание

2) Перечислите функции процессов управления

3) Какими принципами руководствуются в управлении СБП

4) На какие группы делят информацию, без которых функционирование службы безопасности невозможно

5) Какие задачи решает кризисная группа и кто входит в её состав

2. Создайте мини-презентацию на тему “Эффективное функционирование службы безопасности”. Презентация должна содержать рекомендации по организации СБ, проектированию, обеспечению охраны и эксплуатации её средств.

САМОСТОЯТЕЛЬНАЯ РАБОТА № 7 “ Организация информационно-аналитической работы”

Краткие теоретические сведения:

Цели и задачи информационно-аналитической работы

Информационно-аналитическая деятельность службы безопасности предприятия представляет собой системное получение, анализ и накопление информации с элементами прогнозирования по вопросам, относящимся к безопасности предприятия, и подготовка рекомендаций руководству о правомерной защите от противоправных посягательств.

Для проведения информационно-аналитической работы в составе службы безопасности предприятия вводится информационно-аналитическое

подразделение (ИАП), представляющее собой комплексную систему анализа, контроля и прогнозирования внешней и внутренней ситуации, складывающейся вокруг предприятия.

Основной задачей ИАС становится информационно-аналитическое обеспечение принятия решений по вопросам основной деятельности предприятия.

При выполнении информационно-аналитической работы необходимо решить следующие задачи:

обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам;

описать сценарии действий конкурентов, которые могут затрагивать текущие интересы предприятия;

осуществлять постоянный мониторинг событий во внешней конкурентной среде и на рынке, которые могут иметь значение для интересов предприятия;

обеспечить безопасность собственных информационных ресурсов;

обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.

Направления и методы аналитической работы

Направления аналитической работы определяются ИАП с учетом конкретных особенности предприятия. К основным направлениям аналитической работы можно отнести анализ объекта защиты, угроз, каналов несанкционированного доступа к информации, комплексной безопасности предприятия, нарушений режима конфиденциальности, а также анализ подозрений утраты конфиденциальной информации. Направления аналитической работы ИАП предприятия могут быть постоянными, периодическими и разовыми.

Постоянные направления аналитической работы являются наиболее важными. Периодические и разовые направления аналитической работы характеризуются своей жесткой зависимостью от постоянных направлений.

Не менее важными являются периодические направления аналитической работы, которые проводятся через определенные промежутки времени с целью контроля эффективности и возможности внесения улучшений в действующую в фирме систему защиты информации.

Разовые направления аналитических исследований также являются очень важными в силу того факта, что бывают вызваны чрезвычайными обстоятельствами, происшествиями, неожиданно появившимися проблемами и требуют проведения исследований в кратчайшие сроки

Каждое предприятие ведет индивидуальные направления аналитической работы и самостоятельно решает, следует ли разрабатывать их постоянно, периодически или только по мере надобности. Направления аналитической работы могут быть различными, но логика взаимодействия и система связей

между направлениями исследований должны сохраняться. Принципиально важными являются ключевые направления, работа по которым ведется постоянно. Такими направлениями, например, является анализ информации для обнаружения каналов НСД. Результаты аналитической работы показывают степень безопасности условий функционирования предприятия и являются основой для построения и совершенствования системы защиты предприятия. Поиск предполагаемого или предотвращение действующего канала НСД к информации возможны только при наличии постоянного контроля и анализа объекта защиты.

Обнаружение каналов НСД к конфиденциальной информации предприятия входит в число постоянных направлений аналитической работы и в общем виде включает в себя:

- анализ источников конфиденциальной информации;
- анализ каналов объективного распространения информации;
- аналитическую работу с источником угрозы информации.

Рассмотрим данные направления более подробно:

Аналитическое исследование источников конфиденциальной информации предусматривает:

- Выявление и классификацию существующих и возможных конкурентов и соперников предприятия, криминальных структур и отдельных преступных элементов;
- Выявление и классификацию максимально возможного числа источников конфиденциальной информации предприятия;
- Выявление, классификацию и ведение перечня реального состава циркулирующей на предприятии конфиденциальной информации;
- Изучение данных учета осведомленности сотрудников в тайне предприятия;
- Ведение и анализ полноты перечня защитных мер, существующих на предприятии.

Аналитическая работа с источником угрозы конфиденциальной информации предусматривает:

- Выявление и классификацию максимального состава источников угрозы конфиденциальной информации;
- Анализ риска возникновения угрозы;
- Разработку превентивных мероприятий по локализации и ликвидации объективных угроз.

Анализ возникновения угроз рекомендуют вести по такой схеме: вначале нужно выяснить, кто является злоумышленником и что ему нужно, затем, исходя из имеющихся у него средств и возможностей, будет гораздо легче спрогнозировать, как именно он попытается достигнуть своей цели.

Анализ угроз является одним из самых важных разделов аналитической работы и представляет собой ответ на вопрос, от чего или кого следует

защищаться. Источники угрозы конфиденциальной информации бывают объективные и субъективные Объективные источники не связаны с человеческим фактором. Однако наличие источника угрозы само по себе не является угрозой. Угроза реализуется в действиях.

Таким образом, наличие, ведение и результаты постоянной аналитической работы определяют структуру и содержание системы защиты информации и направления её совершенствования.

Этапы выполнения информационно-аналитических исследований производственных ситуаций

В настоящее время рекомендуется использовать следующую форму изложения данных аналитического отчета:

1. *Заключение.* Здесь должны содержаться ответы на вопросы, какова степень важности полученной информации, ее значение для принятия конкретных решений, идет ли речь о каких-либо угрозах, подозрениях, выявленных негативных факторах и т.п., какое отношение имеет предмет отчета к другим областям аналитической работы.
2. *Рекомендации.* В этом разделе должны быть указаны конкретные направления дальнейших действий службы безопасности и других структурных подразделений предприятия для улучшения системы безопасности, предотвращения утраты информации, принятия наиболее эффективных решений и т.п.
3. *Обобщение информации.* Здесь излагают самую существенную информацию без излишней детализации.
4. *Источники и надежность информации*. В этом разделе должны быть указаны предполагаемые оценки надежности данных и источника на момент написания отчета, так как для принятия решений необходимо оценить надежность материалов, являющихся их базой.
5. *Основные и альтернативные гипотезы*. Обязательно должны указываться рассмотренные в ходе анализа наиболее вероятные гипотезы, что помогает принимать более взвешенные и адекватные решения, а также позволяет еще раз оценить правильность выбранной гипотезы.
6. *Недостающая информация*. Четко указывается, какая именно дополнительная информация необходима для подтверждения окончательной гипотезы и принятия решения.

Методы выполнения аналитических исследований

Основным назначением всех аналитических методов является обработка полученных сведений, установление взаимосвязи между фактами, выявление значения этих связей и выработка конкретных предложений на основе достоверной и полной, аналитически обработанной информации. Существует широкий спектр специальных методов анализа информации.

С помощью *диаграмм связей* выявляется наличие связи между субъектами, вовлеченными в конкретную ситуацию, подвергающуюся анализу, а также области общения, соприкосновения этих субъектов. На диаграмме связей отмечают как наиболее прочные, так и вспомогательные

связи между субъектами. Для большей наглядности следует также указывать на диаграмме связи должностей (для физических лиц) или род деятельности (для юридических лиц).

Матрицы связей отражают частоту взаимодействия субъектов за определенный период времени. Такой метод анализа дополняет диаграммы связей, позволяет оценить характер взаимодействий между субъектами через частоту таких взаимодействий.

Схемы потоков информации позволяют оценить то, каким образом происходят события.

Временные графики используются для регистрации событий. Такая форма представления данных помогает не только эффективнее анализировать события, но и более рационально планировать меры противодействия.

В последнее время для аналитической работы все чаще применяются так называемые *экспертные системы*. Такие системы представляют собой класс компьютерных программ, которые выдают советы, проводят анализ, выполняют классификацию, иногда могут объяснить аналитику причину той или иной последовательности действий.

Задание:

1. Ответить на вопросы:

1) Задачи информационно-аналитического подразделения
2) Основные направления аналитической работы
3) На какие временные группы можно разделить направления аналитической работы
4) В каких направлениях ведутся работы для предотвращения НСД
5) Основные формы изложения данных аналитического отчета
6) Методы выполнения аналитических исследований

2. Подготовьте доклад на тему “Методика построения (аналитического обследования) системы информационной безопасности предприятия”

САМОСТОЯТЕЛЬНАЯ РАБОТА № 8 “Организация работы с персоналом предприятия”

Краткие теоретические сведения:

Подбор и подготовка кадров

В настоящее время стало очевидным, что без активного вовлечения в процесс обеспечения информационной безопасности предприятия всех сотрудников, имеющих доступ к конфиденциальной информации, результат не может быть полным. Специалисты по защите информации приводят данные, утверждающие, что определяющей фигурой в обеспечении сохранности ценных сведений предприятия является его сотрудник.

Анализ угроз информации позволил выделить следующие виды угроз информационным ресурсам, которые могут исходить от людей различных групп. по возрастании степени опасности информационным ресурсам, исходящей от них, выделяют следующие группы:

некомпетентные служащие;

хакеры и крэкеры;

неудовлетворенные своим статусом служащие;

нечестные служащие;

инициативный шпионаж;

организованная преступность;

политические диссиденты;

террористические группы.

С учетом этого представляется целесообразным с целью обеспечения информационной безопасности предприятия уделять большее внимание подбору и изучению кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи.

При профотборе сотрудников для работы на коммерческих предприятиях рекомендуется придерживаться следующих этапов процедуры отбора персонала:

Первый этап. Предварительное собеседование.

На этом этапе осуществляется предварительная беседа, которая реализуется в нескольких вариантах и может носить как поверхностный, так и углубленный характер. При поверхностном собеседовании в основном ограничиваются уточнением отдельных, наиболее значимых сведений и постановкой нескольких, совершенно конкретных вопросов. Такое собеседование проводиться, как правило, в случаях массового отбора кандидатов.

Первую ознакомительную беседу следует проводить по стандартной формализованной форме, что позволяет в дальнейшем осуществлять компьютерную обработку ответов кандидата и достаточно быстро получать обобщенные результаты собеседования.

Практика показывает, что предварительные беседы с лицами, принимаемыми на работу, могут использоваться для добывания через них информации о предприятиях, где они работали ранее, конкурентах, о состоянии рынка и т.д.

Для избежание подобных недоразумений следует в самом начале встречи четко и однозначно уточнить вопрос о подписании кандидатом каких-либо внутренних документов на прежнем рабочем месте, обязывающих его соблюдать режим неразглашения коммерческой тайны.

Второй этап. Сбор и оценка информации о кандидатах.

На этом этапе осуществляется углубленная оценка личных и деловых качеств кандидата на работу. При этом для служб безопасности предприятия представляется наиболее важным добывание сведений биографического характера не только на проверяемое лицо, но и его родственников, а также выявление дружеских, служебных и родственных связей.

Затем в ходе этого этапа на основе анализа документов, представленных самим кандидатом, а также данных, полученных через отдел кадров и службу безопасности, выявляются кандидаты, с которыми есть смысл вести дальнейшую работу, а также те, которые явно не соответствуют требованиям, предъявляемым к будущим сотрудникам.

По некоторым данным зарубежных и российских коммерческих служб, и агентств, осуществляющих подбор персонала, уже на этом этапе отпадает, как правило, от 10 до 30% претендентов.

Третий этап. Тестовые примеры и иные научные методики проверки кандидатов.

Этот этап характеризуется тем, что кандидат подвергается комплексными психологическими тестированиями. В настоящее время используются многочисленные методы и процедуры персонального очного тестирования, поскольку они характеризуются быстротой реализации и достаточно высокой эффективностью. Следует иметь в виду тот факт, что каждый из этих методов имеет определенные ограничения, нарушения, которые способны серьезно исказить полученные результаты.

Обычно тестовые методики подразделяются на четыре большие группы.

Личностные опросные листы. Тесты данного класса представляют собой перечни вопросов, которые требуют от испытуемых лиц однозначно выразить согласие или несогласие с их содержанием. После тестирования ответы анализируются по специальному алгоритму оператором-психоаналитиком. На основе полученных данных формируются психологические характеристики испытуемых претендентов. К таким тестам относятся: тест СМИЛ, тест Кеттела, тест Азенка, тест РСК, тест КУСОРТ, тест Томаса и тест УСК.

Бланковые методики. Эти процедуры представляют собой наборы заданий различной степени сложности, которые предъявляются испытуемому лицу на карточках либо бланках. Кандидат должен найти правильный ответ,

выбрав его из предлагаемых ему вариантов, или предложить свой индивидуальный вариант решения задачи. Подобные тесты используются для оценки так называемого "индекса интеллекта" либо степени сформированности отдельных психофизиологических функций. К подобным методикам относятся в первую очередь тесты Равена, Векслера, методика компасов, таблица Шульца и другие.

Проективные методики. Эти процедуры представляют собой еще более усложненный тип тестов. Полученные с их помощью результаты могут быть достоверно интерпретированы лишь за редким исключением только специалистами, имеющими большой опыт работы с этими методиками. К этой группе тестов относятся цветовой тест Люшера, пятна Рорхана, тест Розенцвейга.

Приборные методики – это комплексные процедуры с использованием сложных технических устройств, которые предназначены для всесторонней оценки психофизиологических характеристик испытуемых лиц. В российской практике профессионального отбора кандидатов на работу в коммерческие структуры подобные методики используются пока еще редко, поскольку для их реализации требуются специальные помещения, оборудование и специалисты-психофизиологи.

Четвертый этап. Исследование результатов тестирований.

На этом этапе выполняется аналитическая обработка и комплексный анализ результатов тестирований. данный этап при профотборе является наиболее ответственным, поскольку именно от него во многом зависит успех всей предшествующей работы.

В настоящее время обработка материалов тестирования осуществляется с использованием ЭВМ, что значительно ускоряет этот процесс и позволяет избегать ошибок, снижает вероятность субъективных оценок.

Объективно и всесторонне оценивая существующие тестовые методики, необходимо подчеркнуть следующее: их специфика сегодня такова, что получить однозначный ответ о надежности будущего сотрудника пока все еще не предоставляется возможным. С помощью тестирований достигается лишь возможность сформулировать весьма полный набор характеристик изучаемого кандидата. При этом их глубина и точность в значительной мере зависят от использования пакета методик, а также от тщательности соблюдения операторами инструкций по тестированию и, конечно, их квалификации, опыта, знания характерных особенностей тестируемого контингента сотрудников.

При сравнительном анализе нескольких кандидатур рекомендуется придерживаться следующей последовательности:

- определение среди кандидатов тех лиц, которые по своим психологическим параметрам явно не подходят для планируемой работы;

- выявление среди тестируемого контингента тех лиц, в отношении которых можно высказать весьма обоснованные подозрения о наличии у них каких-либо психических нарушений;

- фиксирование тех кандидатов, которые не обладают качествами, противопоказанными для принятия на работу, хотя при этом профессионально значимые черты пока не сформированы либо сформированы, но в недостаточной степени;

- выделение из группы кандидатов тех лиц, которые по своим психологическим характеристикам соответствуют требованиям профессиограммы полностью или частично.

Таким образом, всех кандидатов по ряду формальных признаков можно разделить на четыре основные группы. С тестируемыми лицами, попавшими в первую и вторую группы, дальнейшая работа не целесообразна. Из состава третьей группы в дальнейшем на собеседования можно приглашать тех, чьи психологические характеристики позволяют предполагать быстрое развитие у этих лиц профессионально значимых качеств. Членов четвертой группы рекомендуется практически без исключения допускать ко второму собеседованию.

Пятый этап. Заключительное собеседование.

Итоговое собеседование является основным этапом приема кандидата на работу. Опыт показывает, что именно на данном этапе сотрудники кадровых аппаратов и руководители предприятий допускают наибольшее количество ошибок. Их главная причина кроется в том, что к самому факту собеседования относятся, как правило, формально. Имеется в виду то обстоятельство, что к данному моменту решение либо уже в целом принято, либо сформировано на 90-95%. Именно поэтому заключительная беседа с кандидатом сводится зачастую к уточнению лишь некоторых второстепенных вопросов и порой к окончательному согласованию отдельных пунктов трудового договора.

Перед началом заключительного собеседования рекомендуется составить примерный план беседы, обычно включающий следующие основные пункты:

- выделение основных вопросов, требующих уточнения и разъяснения, итоги которых способны повлиять на окончательное решение о приеме кандидата на работу. Например, выявление истинного стремления поступить на работу, трудно объяснимая глубокая осведомленность о характере будущей деятельности, криминальные либо сомнительные причины увольнения с прежнего места работы;

- прогнозирование вероятного поведения представителей кадровой службы и руководства, если в ходе собеседования вскроются новые и неожиданные обстоятельства, ставящие под сомнение возможность зачисления кандидата на работу;

- выбор оптимального времени, продолжительности, места проведения собеседования, которые должны быть удобными и приемлемыми для обеих сторон.

Выделяют три этапа заключительной беседы.

Начальный этап собеседования. В подобной беседе большое значение приобретает начальная фаза общения представителя предприятия с кандидатом.

Заключительное собеседование рекомендуется начинать с обсуждения нейтральных тем и вести его, проявляя дружелюбие и максимальное внимание к собеседнику, рассматривая его в качестве вероятного кандидата на работу. На этой же стадии желательно ознакомить кандидата с некоторыми официальными документами, рекламными материалами, образцами, которые бы позволили ему сформировать собственное представление о данной организации. На этом вступительная часть беседы обычно завершается.

Структура содержания центральной части собеседования. Наиболее ответственной является основная часть беседы. Ее следует строить таким образом, чтобы кандидат отвечал на поставленные вопросы развернутыми предложениями, отражая в них те аспекты своей биографии, которые представляются важными для данного коммерческого предприятия. К числу наиболее значимых вопросов этой фазы собеседования традиционно относят следующие:

- основные побудительные мотивы, по которым кандидат решил предложить свои услуги данному предприятию;

- перспективные планы кандидата;

- отрицательные моменты, которые возникали по месту предыдущей работы кандидата;

- личные и деловые связи, характер отношений с руководителями и сотрудниками на предыдущем месте работы.

При оценке ответов кандидата на вопросы представляется возможным достаточно глубоко оценить продуманность, устойчивость и окончательный характер решения кандидата.

Завершение итоговой беседы. Если в ходе собеседования не удалось выявить каких-либо фактов, которые бы делали сомнительным вопрос о приеме кандидата на работу, рекомендуется переходить к заключительному этапу - подписанию трудового контракта или договора. Эту часть беседы целесообразно проводить в официальной обстановке. Кандидату на работу следует предоставить возможность тщательно ознакомиться с текстом соглашения, особенно в части, касающейся его персональных обязательств перед данной коммерческой структурой.

Заключение контрактов и соглашений о секретности

Обязательство о неразглашении конфиденциальной информации и сохранении тайны фирмы претендент подписывает до того, как ему будет

сообщен состав ценных сведений, с которыми ему предстоит работать, и порядок защиты этих сведений.

Обязательство (подписка, соглашение) о неразглашении конфиденциальных сведений представляет собой правовой документ, которым претендент добровольно и письменно дает согласие на ограничение его прав в отношении использования конфиденциальной информации. Одновременно в обязательстве претендент предупреждается об ответственности за разглашение этой информации.

Обычно при составлении подобного соглашения включают следующие пункты:

- детальное изложение принципов определения конкретных сведений, составляющих тайну фирмы;
- краткое изложение порядка охраны конфиденциальных сведений;
- изложение мер, которые должен принимать сам работник для обеспечения сохранности этих сведений;
- перечень административных наказаний, которым может быть подвергнут работник, разгласивший сведения, составляющие тайну фирмы.

Договорные обязательства подписывают не только претенденты на работу на данном предприятии, но и все лица, потенциально имеющие возможность узнать элементы тайны фирмы (акционеры, партнеры). Подписание обязательства о неразглашении тайны фирмы следует предусмотреть и для сотрудников предприятия, которые не имеют непосредственного отношения к закрытым сведениям, однако имеют возможность ознакомиться с ними при исполнении служебных обязанностей (шоферы, дворники, уборщицы, сотрудники охраны, и др.).

Считается, что обязательство о неразглашении тайны фирмы не дает полной гарантии сохранения этих сведений, однако, как показывает практика, существенно снижает риск разглашения персоналом или иными лицами этих сведений, риск незаконного их использования, а также число попыток конкурентов внедрить на фирму свою агентуру.

После подписания обязательства и проведения беседы-инструктажа с кандидатом заключается трудовой договор или контракт. В контракте должен быть пункт об обязанности работника не разглашать сведения, составляющие тайну предприятия, а также конфиденциальные сведения партнеров и клиентов. В контракт может быть включен пункт о собственности предприятия на результаты работы сотрудника, на сделанные им изобретения и открытия. В обязательном порядке включается пункт об обязанности сотрудника немедленно сообщать непосредственному руководителю и службе безопасности об утере носителей конфиденциальной информации, документов, дел, конфиденциальных материалов, изделий и т.п. В заключительной части контракта указывается степень ответственности за разглашение тайны фирмы или несоблюдение правил защиты информации.

После подписания приказа о приеме на работу в отделе кадров формируется личное дело сотрудника, включающее стандартный набор документов.

Особенности увольнения сотрудников, владеющих конфиденциальной информацией

Серьезное влияние на вопросы безопасности коммерческих предприятий оказывают процедуры увольнения сотрудников. К сожалению, отдельных руководителей порой мало интересуют чувства и переживания персонала, который по тем или иным причинам попадает под сокращение или самостоятельно изъявляет желание покинуть предприятие. опыт показывает, что такой подход приводит к серьезным негативным последствиям.

Современные психологические подходы к процессу увольнения позволяют выработать следующую принципиальную рекомендацию: каковы бы ни были причины увольнения сотрудника, он должен покидать коммерческую организацию без чувства обиды, раздражения. Только в этом случае можно надеяться на то, что увольняемый сотрудник не предпримет противоправных необдуманных действий из чувства мести.

Таким образом, представители кадровых подразделений и служб безопасности должны быть четко ориентированы на выяснение истинных мотивов увольнения всех категорий сотрудников. Зачастую причины, на которые ссылается сотрудник при увольнении, и подлинные мотивы, побудившие его к такому шагу, существенно отличаются друг от друга.

Поэтому главная задача состоит в том, чтобы определить истинную причину увольнения сотрудника, попытаться правильно ее оценить и решить, целесообразно ли в данной ситуации предпринимать попытки к искусственному удержанию данного лица в коллективе либо отработать и реализовать процедуру его спокойного и бесконфликтного увольнения.

При поступлении устного или письменного заявления об увольнении рекомендуется во всех без исключения случаях провести с сотрудником беседу с участием руководства предприятия. Однако до беседы целесообразно предпринять меры по сбору следующей информации об увольняемом сотруднике:

- характер его взаимоотношений с коллегами в коллективе;
- отношение к работе;
- уровень профессиональной подготовки;
- наличие конфликтов личного или служебного характера;
- ранее имевшие место высказывания или пожелания перейти на другое место работы;
- доступ к информации, в том числе составляющей коммерческую тайну;
- вероятный период устаревания сведений, составляющих коммерческую тайну для данного предприятия;
- предполагаемое в будущем место работы увольняющегося сотрудника.

В зависимости от предполагаемого результата беседа может проводиться в официальном тоне либо иметь форму доверительной беседы, задушевного разговора, обмена мнениями. Однако каковы бы ни были планы в отношении данного сотрудника, разговор с ним должен быть построен таким образом, чтобы последний ни в коей мере не испытывал чувства униженности, обиды, оскорбленного достоинства. Если руководством предприятия все же

принято решение не препятствовать увольнению сотрудника, а по своему служебному положению он располагал доступом к конфиденциальной информации, то в этом случае отрабатывается несколько вариантов сохранения в тайне коммерчески сведений. Так, оформление официальной подписи о неразглашении данных, составляющих коммерческую тайну, либо устная договоренность о сохранении увольняемым сотрудником секретов предприятия.

В тех случаях, когда увольнения сотрудников происходят по инициативе предприятия, рекомендуется действовать следующим образом. В этих обстоятельствах не следует поспешно реализовывать принятое решение. Если увольняемое лицо располагает какими-либо сведениями, составляющими коммерческую тайну, то нужно предварительно и под благовидными предлогами перевести его на другой участок работы в такое подразделение, в котором отсутствует подобная информация. Кроме того, таких лиц традиционно стремятся сохранить в структуре предприятия до тех пор, пока не будут приняты меры к снижению возможного ущерба от разглашения ими сведений, составляющих коммерческую тайну, либо найдены адекватные средства защиты конфиденциальных данных.

Только лишь после реализации этих мер рекомендуется приглашать на собеседование подлежащего увольнению сотрудника и объявлять конкретные причины, по которым предприятие отказывается от его услуг. После объявления об увольнении рекомендуется внимательно выслушать доводы, аргументы и замечания сотрудника в отношении характера работы, стиля руководства и т д. Если подходить не предвзято и объективно к подобной критике, то эти соображения могут быть использованы в дальнейшем весьма эффективно в интересах предприятия.

При окончательном расчете обычно рекомендуется поблагодарить сотрудника за работу и независимо от личных характеристик увольняемых сотрудников взять у него подписку о неразглашении конфиденциальных сведений, ставших известными в процессе работы.

В любом случае после увольнения сотрудников, осведомленных о сведениях, составляющих коммерческую тайну, целесообразно используя возможности службы безопасности предприятия или частного детективного агентства проводить контроль за ними по их новому месту работы и прогнозировать возможности утечки конфиденциальных данных.

Задание:

1. Ответить на вопросы:

1) Назовите основные этапы профотбора сотрудников

2) Назовите группы людей, от которых могут исходить угрозы информационным ресурсам предприятия

3) Какие тестовые методики применяют при профотборе

4) Какова структура заключительного собеседования

5) В чем заключаются особенности увольнения сотрудников, владеющих конфиденциальной информацией предприятия

2. Подготовьте доклад на тему:

1) тест СМИЛ
2) тест Кеттела
3) тест Азенка
4) тест РСК
5) тест КУСОРТ
6) тест Томаса
7) тест УСК

ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

1.1. Введение. Цель, задачи, содержание и структура дисциплины

1.2. Структура службы информационной безопасности

Техника защиты информации. Защита информации [Текст] : требования к средствам высоконадежной биометрической аутентификации / Федеральное агентство по техническому регулированию и метрологии, Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому экспортному контролю (ГНИИИ ПТЗИ ФСТЭК России), Технический комитет по стандартизации ТК 362 "Защита информации". - Изд. офиц.введен впервые, введен 27.12.2006. - М. : Стандартинформ, 2007. - 19 с. - (Национальный стандарт РФ).

Информационная технология. Методы и средства обеспечения безопасности [Текст] . - Изд. офиц. - М. : Стандартинформ, 2007 - (Национальный стандарт РФ).

1.3. Функции основных групп службы безопасности

Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (541 КБ). - Курск : ЮЗГУ, 2017. - 16 с. : ил., табл. - Библиогр.: с. 16.

Работа с нормативно-правовыми документами [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (212 КБ). - Курск : ЮЗГУ, 2017. - 11 с. : табл. - Библиогр.: с. 11.

1.4. Минимальный штатный состав СБ и обязанности сотрудников

Организация производства и управление предприятием [Текст] : учебник / под ред. О. Г. Туровца. - 2-е изд. - М. : ИНФРА-М, 2008. - 544 с. - (Высшее образование). - ISBN 978-5-16-0021 53-9

1.5. Цели и задачи СБИ

Информационная технология. Методы и средства обеспечения безопасности [Текст] . - Изд. офиц. - М. : Стандартинформ, 2007 - (Национальный стандарт РФ).

Методы и средства обеспечения безопасности [Текст] : информационная технология. - Изд. офиц. - М. : Стандартинформ, 2007 - (Национальный стандарт РФ).

1.6. Функции службы защиты информации

Информационная технология. Методы и средства обеспечения безопасности [Текст] . - Изд. офиц. - М. : Стандартинформ, 2007 - (Национальный стандарт РФ).

Методы и средства обеспечения безопасности [Текст] : информационная технология. - Изд. офиц. - М. : Стандартинформ, 2007 - (Национальный стандарт РФ).

1.7. Организация деятельности службы безопасности

Организация производства и управление предприятием [Текст] : учебник / под ред. О. Г. Туровца. - 2-е изд. - М. : ИНФРА-М, 2008. - 544 с. - (Высшее образование). - ISBN 978-5-16-0021 53-9

1.8. Организационные основы и принципы деятельности службы

Основы управленческой деятельности: управление персоналом, управленческая психология, управление на предприятии [Текст] : учебник / В. Г. Шипунов, Е. Н. Кишкель. - 2-е изд., перераб. и доп. - М. : Высшая школа, 2000. - 304 с. : ил. - ISBN 5-06-003498-4

1.9. Пакет документов для СИБ Правоведение [Текст] : учебник / М. Б. Смоленский. - 2-е изд. - Москва : РИОР : ИНФРА-М, 2015. - 430 с. - (Высшее образование - Бакалавриат). - Библиогр.: с. 428-429. - ISBN 978-5-369-01382-3 (РИОР) (в пер.). - ISBN 978-5-16-010229-0 (ИНФРА-М)

1.10. Лицензирование видов деятельности службы безопасности предприятия.

Правоведение [Текст] : учебник / М. Б. Смоленский. - 2-е изд. - Москва : РИОР : ИНФРА-М, 2015. - 430 с. - (Высшее образование - Бакалавриат). - Библиогр.: с. 428-429. - ISBN 978-5-369-01382-3 (РИОР) (в пер.). - ISBN 978-5-16-010229-0 (ИНФРА-М)

1.11. Управление службой защиты информации. Методы управления

Информационная технология. Методы и средства обеспечения безопасности [Текст] . - Изд. офиц. - М. : Стандартинформ, 2007 - . - (Национальный стандарт РФ).

1.12. Управление СЗИ. Принципы управления

Управление персоналом организации [Текст] : учебник / Под ред. А. Я. Кибанова. - М. : ИНФРА-М, 1998. - 512 с. - ISBN 5-86225-328-9

1.13. Управление СЗИ. Функции процессов управления

Управление персоналом организации [Текст] : учебник / Под ред. А. Я. Кибанова. - М. : ИНФРА-М, 1998. - 512 с. - ISBN 5-86225-328-9

1.14. Организация информационно-аналитической работы. Цели

Организация производства и управление предприятием [Текст] : учебник / под ред. О. Г. Туровца. - 2-е изд. - М. : ИНФРА-М, 2008. - 544 с. - (Высшее образование). - ISBN 978-5-16-0021 53-9

1.15. Организация информационно-аналитической работы. Этапы

Основы управленческой деятельности: управление персоналом, управленческая психология, управление на предприятии [Текст] : учебник / В.

Г. Шипунов, Е. Н. Кишкель. - 2-е изд., перераб. и доп. - М. : Высшая школа, 2000. - 304 с. : ил. - ISBN 5-06-003498-4

1.16. Организация работы с персоналом предприятия

Организация производства и управление предприятием [Текст] : учебник / под ред. О. Г. Туровца. - 2-е изд. - М. : ИНФРА-М, 2008. - 544 с. - (Высшее образование). - ISBN 978-5-16-0021 53-9

Основы управленческой деятельности: управление персоналом, управленческая психология, управление на предприятии [Текст] : учебник / В. Г. Шипунов, Е. Н. Кишкель. - 2-е изд., перераб. и доп. - М. : Высшая школа, 2000. - 304 с. : ил. - ISBN 5-06-003498-4

Управление персоналом организации [Текст] : учебник / Под ред. А. Я. Кибанова. - М. : ИНФРА-М, 1998. - 512 с. - ISBN 5-86225-328-9

Персонал [Текст]. - М. : Знание & дело, 2007. - ISBN 5-902362-06-7 :