# Лабораторная работа №4. Создание организационной подсистемы информационной безопасности предприятия

## Цель работы

Освоить методику оформления организационно-распорядительных документов, регламентирующих работу по защите информации в организации.

## Теоретическая часть

Организационная защита информации является основой и важнейшим элементом в общей системе защиты информации предприятия, с высокой эффективностью обеспечивающим ее защиту при условии соблюдения должностными лицами предприятия норм и правил защиты информации, определенных в соответствующих нормативно-методических документах.

Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и программно-аппаратные) реализовать на практике спланированные руководством предприятия меры по защите информации.

Цель принимаемых руководством предприятия и должностными лицами организационных мер — исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.

Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

Используются два примерно равнозначных определения организационной зашиты информации.

***Организационная защита информации*** — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

***Организационная защита информации на предприятии*** — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

К основным организационным мероприятиям относят:

1. Организацию режима и охраны. Их цель - исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей.
2. Организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил ЗИ.
3. Организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.
4. Организацию использования ТС средств сбора, обработки, накопления и хранения конфиденциальной информации.
5. Организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты.
6. Организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Комплексная система защиты информации любой организации строится на базе организационно-распорядительных документов, которые в свою очередь являются элементом подсистемы организационной защиты информации.

Типовая структура организационно-нормативной документации включает в себя следующие документы:

− «Политика безопасности предприятия», предназначен для определения целей и принципов информационной безопасности. Он так же фиксирует перечень объектов информационной безопасности предприятия, а также список необходимых для ее обеспечения внутренних документов. Обычно оформляется в виде положения. Составляется подразделением, отвечающим за безопасность предприятия. Утверждается руководителем предприятия. Актуализируется не реже 1 раза в год или при изменении состава информационных средств.

− «Распределение ответственности за обеспечение безопасности», предназначен для определения ресурсов информационной безопасности и ответственности за доступ к ним. Оформляется в виде распоряжения. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после изменения политики безопасности или после изменения технологических участков и состава информационных ресурсов.

− «Процесс внедрения новой информационной системы», предназначен для описания процесса внедрения новой информационной системы в действующий бизнес-процесс. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после изменения политики безопасности предприятия.

− «Инвентаризация ресурсов», предназначен для определения категорий ресурсов, подлежащих инвентаризации. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается

руководителем предприятия. Актуализируется не реже 1 раза в год, перед проведением инвентаризации.

− «Классификация ресурсов», предназначен для классификации ресурсов с точки зрения безопасности. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется не реже 1 раза в год.

− «Безопасность при выборе персонала и работе с ним», предназначен для определения мер по обеспечению безопасности при выборе персонала и работе с ним. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками.

− «Реагирование на инциденты в области безопасности, а также на сбои и неисправности», предназначен для определения порядка реагирования на инциденты в области безопасности, на сбои и неисправности информационных систем. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после возникновения инцидентов, сбоев, неисправностей, а также по необходимости.

− «Должностные инструкции по информационной безопасности», предназначен для установки прав и обязанностей, касающихся информационной безопасности, которые должны быть включены в должностные инструкции сотрудников. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− «Процедуры реагирования в случае инцидентов», предназначен для определения порядка реагирования персонала предприятия на возникающие в процессе работы инциденты. Оформляется в виде инструкции. Составляется

подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− «Защита от вредоносного ПО (вирусов, троянских коней)», предназначен для определения правил и способов защиты информационных средств от вредоносного ПО. Оформляется в виде инструкции. Составляется подразделением безопасности и подразделением информатизации предприятия. Утверждается руководителем предприятия. Актуализируется при изменении состава информационных ресурсов.

− «Безопасность носителей данных», предназначен для определения правил работы с носителями информации. Оформляется в виде инструкции. Составляется подразделением безопасности. Утверждается руководителем предприятия. Актуализируется по необходимости.

Методические документы, на базе которых проводится разработка пакета организационно-нормативной документации:

* Российское законодательство;
* стандарты в области информационной безопасности РФ и рекомендации регулирующих органов;
* отраслевые стандарты;
* система технических регламентов;
* нормативные документы национальной системы стандартизации;
* ГОСТы по стандартизации;
* требования ФСБ России, ФСТЭК России, МВД и Минобороны;
* международные стандарты (такие как ISO 27001, ISO 27002 и др.).

## Порядок выполнения работы

Для организации из лабораторной работы №1 разработать пакет организационно-распорядительных документов:

− Положение «Политика безопасности предприятия»;

− Распоряжение о распределении ответственности за обеспечение безопасности;

− Инструкцию по внедрении новой информационной системы;

− Инструкцию по инвентаризации ресурсов;

− Заключение соглашения о соблюдении режима информационной безопасности со всеми сотрудниками;

− Инструкция о порядке реагирования на инциденты в области информационной безопасности, а также на сбои и неисправности;

− Инструкцию по защите от вредоносного ПО (вирусов, троянских коней);

− Инструкцию о безопасности носителей данных.

Состав организационно-распорядительных документов приводится в приложении.

## Контрольные вопросы

СБ?

1. Каким законом регулируются вопросы создания и деятельности частных
2. Кем выдаются лицензии на осуществление частной детективной и

охранной деятельности?

1. Какое оружие и специальные средства могут применяться при осуществлении частной охраной деятельности?
2. Могут ли частные охранники использовать специальные технические средства, предназначенные для негласного получения информации?
3. Правовые основы использования специальных технических средств сбора и защиты информации?
4. Цели и задачи организационной защиты информации, ее связь с правовой защитой информации.
5. Виды угроз информационной безопасности объекту зашиты.
6. Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве.
7. Понятия допуска к секретной (конфиденциальной) информации
8. Понятие доступа к (конфиденциальным) работам, документам и изделиям. 11 Организация работ по защите информации при опубликовании открытых

материалов.

1. Обеспечение режима секретности при хранении и транспортировке объектов.
2. Назначение и требования внутриобъектового режима. 14 Цели и задачи пропускного режима.
3. Порядок оформления и выдачи пропусков.
4. Порядок организации информационной безопасности объекта при осуществлении международного научно-технического и экономического сотрудничества.
5. Организация обеспечения режима секретности при проведении служебного совещания.
6. Планирование работ по защите информации в организации

# Приложение А

## Состав организационно-распорядительных документов

А.1. Документ «Политика безопасности предприятия». Состав документа:

Определение информационной безопасности, перечень ее составляющих.

Определить понятие информационной безопасности, перечислить объекты информационной безопасности предприятия.

Краткое разъяснение политики безопасности, принципов ее построения и соответствия стандартам и требованиям, имеющим особое значение для организации.

Разъяснение соответствия положений политики местному и международному законодательству.

Требования по обучению персонала вопросам безопасности.

Требования по обнаружению и блокированию вирусов и других вредоносных программ.

Требования обеспечения непрерывность ведения бизнеса. Ответственность за нарушения политики безопасности.

А.2. Документ «Распределение ответственности за обеспечение безопасности» Состав документа:

Определение ресурсов, имеющих отношение к информационной безопасности, по каждой системе.

Для каждого ресурса (или процесса) должен быть назначен ответственный сотрудник из числа руководителей. Разграничение ответственности должно быть закреплено документально.

Разграничение ответственности определяется отдельным Приказом или Распоряжением по предприятию.

Для каждого ресурса должен быть определен и закреплен документально список прав доступа (матрица доступа).

А.3. Документ «Процесс внедрения новой информационной системы» Состав документа:

Соответствие новой системы существующей политике управления пользователями.

Проверка всех внедряемых компонентов на совместимость с существующими частями системы.

А.4. Документ «Инвентаризация ресурсов» Состав документа.

### Информационные ресурсы

Базы данных и файлы данных, системная документация, пользовательская документация, учебные материалы, инструкции по эксплуатации или по поддержке,

планы по поддержанию непрерывности бизнеса, мероприятия по устранению неисправностей, архивы информации или данных

### Программные ресурсы

Приложения, операционные системы и системное программное обеспечение, средства разработки

### Физические ресурсы

Вычислительная техника, коммуникационное оборудование (маршрутизаторы, телефонные станции, факсы, автоответчики, модемы), магнитные носители (кассеты и диски), другое техническое оборудование (источники питания, кондиционеры).

А.5. Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками

Условия трудового соглашения с работником

* письменная формулировка их должностных обязанностей
* письменная формулировка прав доступа к ресурсам компании (в том числе и информационным)
* соглашение о конфиденциальности
* специальные соглашения о перлюстрации всех видов служебной корреспонденции (мониторинг сетевых данных, телефонных переговоров, факсов и т.д.).

Включение задачи обеспечения безопасности в служебные обязанности всех сотрудников.

А.6. Документ «Реагирование на инциденты в области безопасности, а также на сбои и неисправности»

Предназначен для определения порядка реагирования на инциденты в области безопасности, на сбои и неисправности информационных систем.

Состав документа:

Отчеты об инцидентах

Отчеты о недостатках в системе безопасности

Отчеты о сбоях и неисправностях компьютерных систем

В случае обнаружения нестандартной ситуации необходимо:

* записать все симптомы ее появления;
* компьютер должен быть изолирован и если возможно его использование приостановлено;
* о факте должно быть немедленно сообщено непосредственному руководителю и службе информационной безопасности, они же должны быть проинформированы о результатах анализа причин произошедшего;

Изучение инцидента

Дисциплинарные меры (в российской специфике это, в зависимости от последствий: дисциплинарные, административные или даже уголовные)

Регулярное обучение персонала по вопросам безопасности

А.7. Документ «Защита от вредоносного ПО (вирусов, троянских коней)» Состав документа.

Состав программных средств.

Обязательность применения только лицензионного программного обеспечения и запрет использования неутвержденного программного обеспечения должны быть закреплены документально

Получение программного ПО Применяемое антивирусное ПО Контроль целостности ПО

Антивирусный контроль входящей информации

Правила восстановления системы после вирусных атак

Мониторинг всей информации, касающейся вредоносного программного обеспечения.

А.8. Документ «Безопасность носителей данных» Состав документа.

Управление съемными носителями

* порядок уничтожения съёмных носителей;
* порядок выноса съёмных носителей за пределы предприятия
* хранение съёмных носителей

Хранение и обращение с носителями

* бумажные документы
* записи на кассетах
* копировальная бумага
* отчеты
* картриджи
* магнитные ленты
* съемные диски или кассеты
* оптические носители
* листинги программ
* тестовые данные
* системная документация

Процедуры обращения с информацией и ее хранения

* учет и маркировка всех носителей
* ограничение доступа
* протоколирование доступа и защита данных из спулинга (например, которые ожидают распечатки).