

Тема 2. Основы информационной безопасности и защиты информации

5. Информационная безопасности в бизнесе



Подходы к доступу к информации в различных организациях



Информационная безопасность предприятия – это комплекс информационно-технических и организационных мер, направленный на:

- ✓ снижение непредвиденных издержек компании,
- ✓ предотвращение утечек конфиденциальной коммерческой информации,
- ✓ предотвращения противоправных действий персонала,
- ✓ поддержание рабочей атмосферы в коллективе,
- ✓ расследования происшествий и противоправных действий,
- ✓ предотвращения утечки персонала,
- ✓ повышение дисциплины и производительности труда,
- ✓ мониторинг уровня лояльности персонала.

Составляющие информационной безопасности

1) Снижение непредвиденных издержек компании.

Это все издержки компании, которые могут возникнуть в результате противоправных действий или бездействий должностных и/или частных лиц, которые могут нанести компании значительный вред и привести к ощутимым потерям.

К таковым следует отнести:

- ухудшение репутации и имиджа компании;
- утрата ноу-хау и секретов (технологических, стратегических и др.);
- ослабление позиций компании в конкурентной борьбе;
- потеря сотрудников;
- уменьшение клиентской базы (снижение притока новых клиентов и уменьшение количества старых клиентов);
- потеря ключевых контрагентов и бизнес-партнеров.

Составляющие информационной безопасности

2) Предотвращение утечек конфиденциальной коммерческой информации.

Под конфиденциальной информацией обычно в общем плане понимают всю ту информацию, потеря которой для организации является нежелательной.



Основные составные части конфиденциальной информации



Составляющие информационной безопасности

3) Предотвращение противоправных действий персонала.

В данном пункте понимаются действия, относящиеся к:

- ❖ активам компании (фин. средства, основные и материальные средства, разработки и ноу-хау компании, персоналу компании);
- ❖ персоналу (дезинформирование, унижение, создание негативного фона в коллективе, способствование увольнению и др.);
- ❖ контрагентам, представителям органов власти, общественности и СМИ (нарушение правил и норм общения, выдача лишней или конфиденциальной информации, дезинформирование, выдача искаженной информации и др.);
- ❖ текущей работе компании (договорные и финансовые документы, условия работы с контрагентами, планирование и отчетность, оплата труда и др.).

Составляющие информационной безопасности

4) Поддержание рабочей атмосферы в коллективе.

Этот пункт как правило касается:

- ❖ предотвращения и расследования конфликтных ситуаций;
- ❖ предотвращения манипулированием сотрудниками;
- ❖ расследования случаев хищения, дезинформирования и распускания слухов;
- ❖ выявления фактов нарушения корпоративной этики и поведения;
- ❖ выявления и работы с неформальными лидерами и лидерами мнений.

Составляющие информационной безопасности

5) Расследования происшествий и противоправных действий.

То есть работа, проводящаяся исключительно постфактум в отношении имевших место фактов.

6) Предотвращения утечки персонала.

Как правило эта деятельность основывается на:

- ❖ выявлении недовольных сотрудников (условиями работы, карьерой, доходом и др.);
- ❖ работа с недовольными сотрудниками (полное или частичное удовлетворение их запросов, разъяснительная работа, ротация или увольнение);
- ❖ выявление фактов сманивания сотрудников (конкурентами, партнерами, бывшими сотрудниками);
- ❖ выявление фактов поиска работы действующих сотрудников.

Составляющие информационной безопасности

7) Повышение дисциплины и производительности труда:

- ❖ выяснение структуры работы в сети персонала (используемые программы и сервисы и их доля времени в работе сотрудников);
- ❖ учет отработанного времени (в разрезе дня, недели, месяца и т.д.);
- ❖ мониторинг входящей и исходящей переписки, а также полученных и отправленных файлов.

8) Мониторинг уровня лояльности персонала.

Этот параметр является «условно сборным», зависящим от производительности и результатов труда сотрудника, а также его исходящего и входящего информационного поля.

Принципы надежной системы информационной безопасности

- 1) Стоимость средств защиты информации должна быть меньше, чем размеры возможного ущерба;
- 2) Каждый пользователь должен иметь минимальный набор привилегий, необходимый для его работы;
- 3) Защита информации тем более эффективна, чем проще пользователю с ней работать;
- 4) Должна быть предусмотрена возможность отключения в экстренных случаях;
- 5) Специалисты, имеющие отношение к системе защиты информации, должны полностью представлять себе принципы ее функционирования и, в случае возникновения затруднительных ситуаций, адекватно на них реагировать;
- 6) Под защитой должна находиться вся система обработки информации;
- 7) Разработчики системы защиты информации не должны быть в числе тех, кого эта система будет контролировать;
- 8) Система защиты информации должна предоставлять доказательства корректности своей работы;

Принципы надежной системы информационной безопасности

- 9) Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность за результат работы системы;
- 10) Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других;
- 11) Надежная система защиты информации должна быть полностью протестирована и согласована;
- 12) Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора;
- 13) Система защиты информации должна разрабатываться исходя из предположения, что пользователи будут совершать серьезные ошибки и вообще имеют наихудшие намерения;
- 14) Наиболее важные и критические решения должны приниматься человеком;
- 15) Существование механизмов защиты информации должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

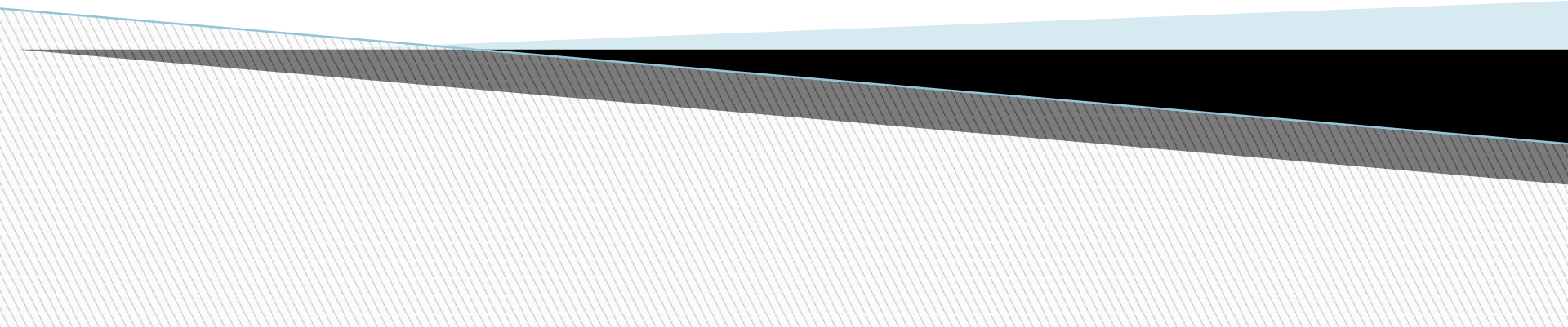


Примерный функционал службы безопасности

- Проверка кандидатов (по базам МВД, проверка документов, поиск отзывов о кандидате, изучение профилей в соц. сетях, проверка на полиграфе);
- Проверка контрагентов (состояние организации, поиск генерального директора в «черном списке» руководителей, поиск отзывов о компании и т.д.);
- Контроль доступа (в помещения, в сеть);
- Видео-охрана (контроль периметра и внутреннее наблюдение);
- Сигнализация (пультовая охрана зданий и помещений);
- Физическая безопасность (осуществление комплекса мер по физической защите отдельных сотрудников);
- Кадровая безопасность (проверки персонала, предотвращение массового оттока и др..

- Защита информации (криптографическая защита, межсетевое экранирование, защита от вирусов, системы обнаружения компьютерных атак, сканирование уязвимостей и др.);
- Экономическая безопасность (контроль сделок, контроль платежей, контроль договорного документооборота и др.);
- Юридическая безопасность (противодействие рейдерству, проверки контрагентов, контроль документооборота и др.);
- Технологическая безопасность (контроль технологической документации и информации).

6. Понятие информационных правоотношений



Информационные правоотношения представляют собой урегулированные нормами информационного права общественные отношения, участники которых выступают как носители юридических прав и обязанностей в информационной сфере.



СУБЪЕКТЫ

Государственные органы,
регулирующие
информационные отношения

Производители информации,
в том числе авторы
(владельцы информации)

Обладатели информации

Потребители информации

ЭЛЕМЕНТЫ ИНФОРМАЦИОННЫХ ПРАВООТНОШЕНИЙ

СОДЕРЖАНИЕ

Права, обязанности и
ответственность субъектов
правоотношений при
осуществлении
информационной
деятельности

Правила поведения
(действие, бездействие)
субъектов при
осуществлении
информационной
деятельности

ОБЪЕКТЫ

Документированная информация

Информационные ресурсы

Информационные продукты

Информационные услуги

Информационные системы

Средства и механизмы обеспечения
информационной безопасности

Классификацию информационных правоотношений можно проводить:

- ❖ по виду информации;
- ❖ на основе анализа информационных процессов в информационной сфере.



Классификация информационных правоотношений

По виду информации информационные правоотношения можно подразделить на три большие группы, имеющие общий характер:

- ❑ правоотношения по поводу информации, которая находится в гражданском обороте (имущественные отношения);
- ❑ правоотношения по поводу информации, которая находится в административном обороте (регулирование общественных отношений, в том числе и в информационной сфере);
- ❑ правоотношения по поводу информации, которая находится в общественном (публичном) обороте (сведения информационного характера или массовая информация).

Классификация информационных правоотношений

На основе анализа информационных процессов в информационной сфере информационные правоотношения можно подразделить на две большие группы:

- ❑ Информационные правоотношения, возникающие при осуществлении поиска, получения и потребления информации;
- ❑ Информационные правоотношения, возникающие при производстве, передаче и распространении информации, информационных ресурсов, информационных продуктов, информационных услуг (данная группа регулируется в зависимости от вида и формы производимой и распространяемой информации и степени ее открытости).

Информационные правоотношения, возникающие при осуществлении поиска, получения и потребления информации.

В этой области *потребители информации* реализуют свое конституционное право на поиск и получение информации любого вида и формы представления за исключением информации ограниченного доступа, порядок получения которой регламентируется особо.

Они несут гражданско-правовую, административно-правовую и уголовную ответственность за неправомерное использование полученной информации.

Потребители вступают в правоотношения с *производителями информации*: государственные организации и органы местного самоуправления или авторы произведений и собственники информационных объектов.

Производители обязаны предоставлять информацию, в указанных законом случаях, и несут ответственность за ее достоверность, полноту и своевременность предоставления.

Информационные правоотношения в области открытой информации

Основные правоотношения, возникающие при обороте открытой информации, связаны защитой личных неимущественных, личных имущественных прав и прав собственности на информационные объекты.

Часть правоотношений, которые возникают при осуществлении органами государственной власти и местного самоуправления обязанностей по информированию потребителя и лицензированию коммерческих организаций, регулируется нормами административно-правового характера.

У производителей открытой информации могут возникать следующие права и обязанности:

- право на создание произведений науки и литературы;
- право интеллектуальной собственности на результаты творческой деятельности и право вещной собственности на документированную информацию, отражающую эти результаты;
- ограничение права на создание документированной информации ограниченного доступа;
- ограничение права на создание вредной, опасной для общества информации;
- обязанность по созданию информационных ресурсов в соответствии с установленной компетенцией и предоставления информации из них потребителям информации;
- обязанность исполнения условий авторских договоров;
- ответственность за непредоставление информации;
- ответственность за недостоверность создаваемой информации, недоброкачественную и ложную информацию и дезинформацию;
- ответственность за качество информационных ресурсов, информационных продуктов, предоставления информационных услуг;
- ответственность за создание и распространение контрафактных экземпляров.

Информационные правоотношения в области массовой информации

У производителей массовой информации могут возникать следующие права и обязанности:

- право на создание массовой информации;
- право на защиту чести и достоинства;
- право интеллектуальной собственности на распространяемые СМИ результаты творческой деятельности;
- обязанность по достоверному, оперативному, полному информированию населения (пользователей Интернет);
- обязанность по обеспечению гарантий свободы слова, ограничение права на распространение информации ограниченного доступа;
- ограничение права на распространение вредной, опасной для общества информации;
- ответственность за недостоверность создаваемой информации, за недоброкачественную и ложную информацию и дезинформацию, за введение цензуры.

Информационные правоотношения в области создания и распространения официальных документов

У производителей официальных документов могут возникать следующие обязанности:

- обязанность по производству и распространению (или обеспечению распространения) нормативных правовых актов в соответствии с установленной компетенцией;
- обязанность за предоставление информации из таких документов;
- ответственность за создание официальных документов неудовлетворительного качества.

Информационные правоотношения в области обязательно представляемой документированной информации

Они возникают при подготовке отчетной и иной представляемой информации, а также выполнении органами исполнительной власти и местного самоуправления своих обязанностей по формированию информационных ресурсов обязательно представляемой документированной информации.

У производителей обязательно представляемой документированной информации могут возникать следующие обязанности:

- обязанность подготовки и представления обязательных документов;
- обязанность по созданию информационных ресурсов, содержащих обязательно представляемую информацию;
- ответственность за использование этой информации исключительно для исполнения установленных законом функций и задач;
- ответственность за недостоверность предоставляемой информации, за недоброкачественную и ложную информацию и дезинформацию.

Информационные правоотношения в области информации ограниченного доступа

Производство, передача и распространение информации ограниченного доступа, формирование и использование информационных ресурсов с такой информацией осуществляются в условиях доступа к ней специально подготовленных и официально допущенных лиц.

Деятельность данных лиц строго регламентирована, а за неправомерные действия с такой информацией, в зависимости от тяжести деяния, наступает административная или уголовная ответственность.



У производителей обязательной информации ограниченного доступа могут возникать следующие обязанности:

- обязанность по установлению состава информации ограниченного доступа;
- обязанность по установлению информации, которая не может относиться к категории ограниченного доступа;
- ограничение имущественных прав при отнесении созданной автором информации к государственной тайне;
- обязанность лицензирования деятельности по обработке информации ограниченного доступа;
- обязанность по установлению ограничений по доступу к информации ограниченного доступа;
- обязанность по обеспечению защиты информации и информационных ресурсов, содержащих такую информацию, от несанкционированного доступа;
- ответственность за нарушение условий ограниченного доступа, за разглашение информации ограниченного доступа.

Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения

В этой области информационные правоотношения между участниками регулируются в основном нормами *гражданско-правового характера*.

Целью правового регулирования является защита личных неимущественных, личных имущественных прав и прав собственности на информационные системы, средства их обеспечения и сети.

В отдельных случаях правовое регулирование осуществляется нормами *административно-правового характера* - при проектировании и эксплуатации государственных информационных систем и средств их обеспечения, а также при лицензировании организаций разработчиков.

Создатели и субъекты, обеспечивающие эксплуатацию таких объектов, несут гражданско-правовую, административно-правовую и уголовную ответственность за создание недоброкачественных технологий и некачественную их эксплуатацию.

У участников информационных правоотношений в данной области могут возникать следующие права и обязанности:

- право на создание и применение информационных систем, их сетей, средств их обеспечения;
- право интеллектуальной собственности на результаты творческой деятельности при создании таких объектов;
- ограничение права на создание таких объектов для информации ограниченного доступа;
- обязанность создания и применения информационных систем, их сетей, средств их обеспечения в соответствии с установленной компетенцией;
- обязанность по заключению и исполнению договоров на создание таких объектов для государственных нужд;
- ответственность за недоброкачеством созданной продукции, нарушение сроков исполнения договора, другие нарушения.

Информационные правоотношения, возникающие при создании и применении средств и механизмов информационной безопасности

К основным объектам, подлежащим защите с помощью средств и механизмов информационной безопасности, относятся:

- интересы гражданина, общества, государства в информационной сфере;
- демократия, знания и духовные ценности общества;
- конституционный строй, суверенитет и территориальная целостность государства;
- информация как интеллектуальная собственность;
- документированная информация, информационные ресурсы, информационные продукты, информационные услуги как интеллектуальная и вещная собственность;
- машинные носители с информацией;
- базы данных (знаний) в составе автоматизированных информационных систем и их сетей;
- программные средства в составе ЭВМ, их сетей, технические средства.

Для субъектов данной группы правоотношений характерны следующие права и обязанности:

- право на защиту личности от воздействия недостоверной, ложной информации;
- право на защиту информации, информационных ресурсов, продуктов от несанкционированного доступа;
- право на защиту интеллектуальной собственности;
- право на защиту информационных систем, информационных технологий и средств их обеспечения как вещной собственности;
- право на защиту информационных прав и свобод;
- ограничение права на раскрытие личной тайны, а также иной информации ограниченного доступа без санкции ее собственника или владельца;
- обязанность по защите государства и общества от вредного воздействия информации, защите самой информации, по защите прав личности, по защите тайны;
- ответственность за нарушение информационной безопасности, в том числе прав и свобод личности, тайны и других ограничений доступа к информации, за компьютерные преступления.

Спасибо за внимание!

