Тема 1. Экономическая безопасность и коммерческая тайна

Литература:
1. Закон Республики Беларусь «О государственных секретах» 19 июля 2010 г. N 170-З
2. Закон Республики Беларусь «Об информации, информатизации и защите информации» 10 ноября 2008 г. N 455-З
3. Закон Республики Беларусь «О коммерческой тайне»

Целью обеспечения экономической безопасности предприятия является ограждение его собственности и сотрудников от источников внешних и внутренних угроз безопасности, предотвращение правонарушений, причин и условий, их порождающих, а также возникновения чрезвычайных ситуаций.
Объектами безопасности (защиты) являются:
■ информация;
■ материальные и финансовые ценности;
■ персонал.
Стратегия экономической безопасности (организации) – это планирование, разработка и организация долгосрочных установок с целью обеспечения безопасности системы.
В зависимости от *категории доступа информация* делится на:
■ общедоступную информацию;
■ информацию, распространение и (или) предоставление которой ограничено.
К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.
Не могут быть ограничены доступ к информации, распространение и (или) предоставление информации:
■ о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;
■ о деятельности государственных органов, общественных объединений;
■ о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;
■ о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;
■ о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;
■ о состоянии преступности, а также о фактах нарушения законности;
■ о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;
■ о размерах золотого запаса;

■ об обобщенных показателях по внешней задолженности;
■ о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь и др.
К информации, распространение и предоставление которой ограничено, относится:
■ информация о частной жизни физического лица и персональные данные;
Сведения, относящиеся к государственным секретам, определены Законом Республики Беларусь от 19.07.2010 N 170-З.
■ сведения, составляющие государственные секреты;
Требования к информации, составляющей коммерческую тайну субъекта хозяйствования, определены постановлением Совета Министров Республики Беларусь от 06.11.1992 N 670.
■ информация, составляющая коммерческую и профессиональную тайну;
профессиональные тайны
врачебная тайна,
адвокатская тайна (вопросы, по которым лицо обратилось за помощью, суть консультаций, советов и разъяснений),
тайна нотариальных действий,
тайна исповеди,
банковская тайна (сведения о счетах, вкладах, об имуществе, находящемся в банке, о конкретных сделках, совершенных клиентом банка).
■ информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;
■ иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.
Государственные секреты (сведения, составляющие государственные секреты) - сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.
К государственным секретам могут быть отнесены:
сведения в области политики:
сведения в области экономики и финансов:
сведения в области науки и техники:
сведения в военной области:
сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:
сведения в информационной и иных областях национальной безопасности Республики Беларусь:
Государственные секреты подразделяются на две категории:
■ государственную тайну (сведения, составляющие государственную тайну) и

■ служебную тайну (сведения, составляющие служебную тайну).

Государственная тайна - сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь.

Служебная тайна - сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь.

Для государственных секретов в зависимости от тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате их разглашения или утраты, устанавливаются *следующие степени секретности*:

■ для государственной тайны - "Особой важности", "Совершенно секретно";

■ для служебной тайны - "Секретно".

Коммерческая тайна - сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям Закона о коммерческой тайне, в отношении которых установлен режим коммерческой тайны.

Режим коммерческой тайны - правовые, организационные, технические и иные меры, принимаемые в целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну.

В соответствии со ст.5 Закона Режим коммерческой тайны может устанавливаться в отношении сведений, которые одновременно соответствуют следующим требованиям:

■ не являются общеизвестными или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобного рода сведениями;

■ имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам;

■ не являются объектами исключительных прав на результаты интеллектуальной деятельности;

■ не отнесены в установленном порядке к государственным секретам.

Сведения имеют коммерческую ценность в случае, если обладание ими позволяет лицу при существующих или возможных обстоятельствах увеличить доходы, сократить расходы, сохранить положение на рынке товаров, работ или услуг либо получить иную коммерческую выгоду.

В соответствии со ст.6 коммерческую тайну не могут составлять сведения:

■ содержащиеся в учредительных документах юридического лица, а также внесенные в Единый государственный регистр юридических лиц и индивидуальных предпринимателей;

■ содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

■ являющиеся врачебной, адвокатской, банковской, налоговой или иной охраняемой законом тайной;

■ о недвижимом имуществе, правах и ограничениях (обременениях) прав на недвижимое имущество, содержащиеся в едином государственном регистре недвижимого имущества, прав на него и сделок с ним;
■ о составе имущества государственных юридических лиц и юридических лиц, акции (доли в уставных фондах) которых принадлежат государству;
об использовании средств республиканского и (или) местных бюджетов;
■ о состоянии окружающей среды, противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих или способных оказать негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и населения в целом;
■ о подлежащих уплате суммах налогов, сборов (пошлин) и других обязательных платежей;
■ о численности и составе работников, об условиях и охране труда, о показателях производственного травматизма и профессиональной заболеваемости, а также о наличии свободных рабочих мест (вакансий);
■ о задолженности нанимателей по выплате заработной платы и по социальным выплатам;
■ о нарушениях законодательства и фактах привлечения к ответственности за совершение этих нарушений;
■ об условиях аукционов (конкурсов) по продаже объектов приватизации и конкурсов по передаче принадлежащих Республике Беларусь или ее административно-территориальной единице акций открытых акционерных обществ в доверительное управление, в том числе с правом выкупа части этих акций по результатам доверительного управления, а также о проданных объектах приватизации, об условиях их продажи и о покупателях;
■ о финансовом состоянии лица, предоставляемые в соответствии с требованиями законодательства об экономической несостоятельности (банкротстве);
■ иные сведения, определенные законодательными актами.
Требования в соответствии с Положением о КТ
Информация, составляющая коммерческую тайну, должна соответствовать следующим требованиям:
■ иметь действительную и потенциальную ценность для субъекта хозяйствования по коммерческим причинам;
■ не являться общеизвестной или общедоступной согласно законодательству Республики Беларусь;
■ обозначаться соответствующим образом с осуществлением субъектом хозяйствования надлежащих мер по сохранению ее конфиденциальности через систему классификации информации как коммерческой тайны, разработки внутренних правил засекречивания, введения соответствующей маркировки документов и иных носителей информации, организации секретного делопроизводства;

■ не являться государственным секретом и не защищаться авторским и патентным правом;
■ не касаться негативной деятельности субъекта хозяйствования, способной нанести ущерб интересам государства.
Законодательством также установлен перечень информации, которая не может быть отнесена к категории коммерческой тайны.
Коммерческую тайну субъекта хозяйствования не могут составлять:
■ учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности;
■ сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;
■ документы о платежеспособности;
■ сведения о численности и составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест.
Содержание и объем информации, составляющей коммерческую тайну, а также порядок ее защиты определяются руководителем субъекта хозяйствования, который доводит их до работников либо лиц, имеющих доступ к таким сведениям.

Тема 2. Интеллектуальная собственность предприятия и ее защита

Литература:
1. Гражданский кодекс Республики Беларусь
2. Зинов В.Г. Управление интеллектуальной собственностью/ В.Г .Зинов. - М.: Дело, 2003. - 512 с.

Интеллектуальная собственность выражает права, относящиеся к интеллектуальной, творческой деятельности человека в производственной, научной, литературной и художественных сферах, а также к изобретениям во всех областях человеческой деятельности, научным открытиям, произведениям литературы, искусства, техники.
Объектами правовой охраны являются те виды результаты интеллектуальной деятельности (РИД), которые определены в соответствующих законах об интеллектуальной собственности.
Объекты правовой охраны РИД и средств индивидуализации юридического лица, продукции, выполненных работ или услуг называют объектами интеллектуальной собственности (ОИС).
К объектам интеллектуальной собственности относятся:
1) результаты интеллектуальной деятельности:
произведения науки, литературы и искусства;
исполнения, фонограммы и передачи организаций вещания;
изобретения, полезные модели, промышленные образцы;
селекционные достижения;
топологии интегральных микросхем;
нераскрытая информация, в том числе секреты производства (ноу-хау);
2) средства индивидуализации участников гражданского оборота, товаров, работ или услуг:
фирменные наименования;
товарные знаки (знаки обслуживания);
географические указания;
и др.

Классификация видов ОИС складывалась исторически и основывается на трех подходах:
- авторское право и промышленная собственность;
- правовая охрана, возникающая на основе обязательной регистрации (объекты патентного права) и без обязательной регистрации в силу создания (объекты авторского права) или при соблюдении специальных условий (топологии интегральных микросхем);
- права на РИД (например, изобретения) и права на средства индивидуализации товаров и товаропроизводителей (например, товарные знаки или фирменные наименования).

Тема 3. Сведения, составляющие коммерческую тайну

Перечень сведений, составляющих коммерческую тайну, утверждается распоряжением генерального директора.

Существуют следующие *подходы к определению* этого *перечня*:

- тотальный;
- плагиаторский;
- аналитический;
- экспертный.

При определении перечня сведений, составляющих коммерческую тайну целесообразно определить:

- какие именно сведения нуждаются в защите;
- кого они могут заинтересовать и какую ценность представляют для конкурентов;
- какие элементы информации являются наиболее важными и уязвимыми;
- как долго сведения, составляющие коммерческую тайну, будут актуальными;
- круг лиц, имеющих право доступа к такого рода сведениям и осуществляющих работу с ними;
- во что обойдется защита информации с финансовой и организационной точки зрения;
- какие условия работы будут необходимы для обеспечения конфиденциальности соответствующей категории сведений.

Методика выделения КТ:

I) проведение анализа всех сторон деятельности предприятия и составление предварительного перечня коммерчески ценной информации предприятия (фирмы).

При составлении *Перечня на основе аналитического подхода* необходимо:

1) выделить те направления деятельности организации, которые приносят прибыль;

2) оценить, исходя из рыночной конъюнктуры сбыта аналогичных товаров, уровень прибыльности по сравнению с другими предприятиями;

3) определить рентабельность организации на перспективу с учетом производства конкретных товаров. Данные о превышении уровня получаемой прибыли по сравнению с выпуском аналогичных товаров на других предприятиях свидетельствуют о необходимости уточнения круга сведений, составляющих коммерческую тайну.

II) исключение из предварительного перечня ценной информации сектора сведений, не соответствующих законодательству.

Примеры сведений, касающихся негативной деятельности и/или наносящей ущерб обществу

- загрязнение окружающей среды;
- нарушение действующих законов;
- неэффективная работа предприятия;

• злоупотребление властью, служебным положением;
• бездеятельность, некомпетентность должностных лиц;
• расточительство;
• уклонение от договорных обязательств;
• недобросовестная конкуренция
III) Ранжирование информации по категориям по стоимостному признаку.

Разработка и утверждение Перечня создает нормативную основу для руководства по определению степени конфиденциальности конкретных сведений, содержащихся в работах, документах и изделиях.
Степень конфиденциальности конкретных сведений определяется непосредственно исполнителем работ на основании соответствующих категорий сведений, предусмотренных в Перечне, и лицом, которому направлен документ на утверждение.
Для определения *степени конфиденциальности КЗИ* (коммерчески значимой информации) Северин В.А. предлагает учитывать следующие критерии и соответствующие им признаки (частные показатели, перечень которых может быть расширен):
1. Характер и относимость информации к защищаемым сферам деятельности организации в зависимости от доступа к ней работников. Они отражены в Примерном перечне (Приложение А) и имеют следующую балльную оценку значимости:
- управление: подготовка и принятие решений по коммерческим, производственным и иным вопросам; планы, совещания, финансы, безопасность и др. (10 баллов);
- научно-исследовательские, опытно-конструкторские, опытно-технологические работы и пр. (8 баллов);
- структура производства, производственные мощности, запасы сырья, комплектующих и т.д., изготовление изделий, применение технологий и др. (6 баллов);
- коммерческая деятельность: рыночная стратегия организации, изучение рынка, партнеры, переговоры, контракты (договоры), цены, торги и др. (5 баллов).
2. Степень важности технической, технологической и деловой информации:
- актуальность сведений (10 баллов);
- новизна сведений (9 баллов);
- обобщенность сведений (7 баллов);
- эффективность технического, технологического и коммерческого решения, оригинальность методов управления (5 баллов).
3. Степень возможности охраны и защиты сведений, составляющих КЗИ:
- уязвимость КЗИ от конкурентной разведки (10 баллов);
- осведомленность конкурентов в КЗИ (9 баллов);
- устремления конкурентов с целью получения КЗИ (8 баллов);
- опасность разглашения КЗИ работниками организации (7 баллов).

Общая оценка степени конфиденциальности информации, циркулирующей в организации, производится (Ок) путем суммирования значения i-го критерия в баллах (pi) и коэффициента значимости i-го критерия (di):

$$Ок = \sum_{i=1}^{3} pi * di \text{ . При этом } \sum_{i=1} di = 1.$$

Рекомендуются следующие значения di: 0,15; 0,35; 0,5.

При выведении общей оценки Ок может быть использована качественная шкала, выраженная в виде разрядов «низкий», «средний», и «высший», означающая степень конфиденциальности информации:

1) открытая информация (доступ не ограничен): значение Ок < 6;
2) гриф «Коммерческая тайна», разряд низкий: Ок = 6–7;
3) гриф «Коммерческая тайна», разряд «средний»: Ок = 7–9;
4) гриф «Коммерческая тайна», разряд «высший»: Ок = 9–10.

В перечень сведений, составляющих коммерческую тайну, могут входить следующие блоки:

- сведения о планировании деятельности предприятия;
- сведения о производственной деятельности предприятия;
- сведения об управлении предприятием;
- сведения о маркетинговой деятельности предприятия;
- сведения о финансовой деятельности предприятия;
- сведения о взаимоотношениях предприятия с контрагентами;
- сведения о научно-технической и иной некоммерческой деятельности предприятия и др.

Тема 4. Утечка информации, содержащей коммерческую тайну

При определенных условиях каналы утечки могут формироваться на *основе каналов распространения информации (стандартных информационных потоков)*.

К таким каналам распространения информации относятся:

■ каналы оперативной связи, существующие в организации.

■ переписка по служебным вопросам, которая ведется в организациях с использованием открытого и конфиденциального делопроизводства.

■ «материальные потоки», образующиеся в процессе производственной и

■ технические каналы,.

■ «внешние окна», позволяющие по косвенным признакам делать выводы о ценности информации.

■ «людские потоки», к которым относят прием и увольнение работников предприятия, посещение предприятия командированными лицами; проведение совещаний по конфиденциальным вопросам; выезд работников за границу; прохождение практики студентами и стажировки аспирантами; посещение международных выставок.

Канал утечки (технический) информации – совокупность, во-первых, источника информации, во-вторых, материального носителя (среды распространения несущего указанную информацию сигнала) и в-третьих, средства выделения информации из носителя (сигнала).

Технические каналы утечки информации принято делить на следующие типы:

■ радиоканалы (электромагнитные излучения радиодиапозона);

■ акустические каналы (распространение звуковых колебаний в любом звукопроводящем материале);

■ электрические каналы (опасные напряжения и токи в различных токопроводящих коммуникациях);

■ оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой части спектра);

■ материально-вещественные каналы (бумага, фото, магнитные носители, отходы и т.д.).

Источники информации характеризуются действительными и потенциальными возможностями, допустимыми пределами использования, степенью надежности.

Для добывания информации конкуренты используют как легальные, так и нелегальные методы.

Американский журнал «Chemical engineering» опубликовал перечень из 16 источников получения информации:

■ сбор информации, содержащейся в средствах массовой информации, включая официальные документы, например, судебные отчеты;

■ использование сведений, распространяемых служащими конкурирующих фирм;

биржевые документы и отчеты консультантов; финансовые отчеты и документы, находящиеся в распоряжении маклеров; выставочные экспонаты и проспекты, брошюры конкурирующих фирм; отчеты коммивояжеров своей фирмы;

- изучение продукции конкурирующих фирм; использование данных, полученных во время бесед со служащими конкурирующих фирм (без нарушения законов);
- замаскированные опросы и «выуживание» информации у служащих конкурирующих фирм на научно-технических конгрессах (конференциях, симпозиумах);
- непосредственное наблюдение, осуществляемое скрытно;
- беседы о найме на работу со служащими конкурирующих фирм (хотя опрашивающий сотрудник вовсе не намерен принимать данного человека в свою фирму);
- так называемые ложные переговоры с фирмой-конкурентом относительно приобретения лицензии;
- наем на работу служащего конкурирующей фирмы для получения требуемой информации;
- подкуп служащего конкурирующей фирмы или лица, занимающегося ее снабжением;
- использование агента для получения информации на основе платежной ведомости фирмы-конкурента;
- подслушивание переговоров, ведущихся в фирмах-конкурентах;
- перехват телеграфных сообщений;
- подслушивание телефонных разговоров;
- кража чертежей, образцов, документации;
- шантаж и вымогательство.

К *легальным методам* относятся:

- изучение публикаций в средствах массовой информации (СМИ);
- участие в научно-технических конференциях;
- анализ общественнополитических, научных и технических изданий;
- посещение выставок; исследование сообщений электронных СМИ (телевидение, радио, интернет) и др.

К законным способам сбора информации конкурентами: относят приобретение и последующий анализ сильных и слабых сторон продукции конкурента.

К *полулегальным методам* можно, в частности, отнести:

- беседы с сотрудниками в неофициальной обстановке;
- мнимые переговоры о покупке продукции;
- ложные конкурсы;
- приглашение на работу ведущих специалистов;
- получение информации от общих поставщиков, потребителей, через фонды и благотворительные организации, через контролирующие органы и др.

Как правило, данные действия могут быть отнесены к актам недобросовестной конкуренции в силу несоответствия нормам и обычаям добросовестной конкуренции.

К *нелегальным методам* относятся:

- похищение образцов продукции и (или) технологического оборудования;
- похищение документов, содержащих интересующую информацию;
- копирование документов, содержащих интересующую информацию;
- внедрение агентов в структуры противника;
- съем информации по техническим каналам;
- проникновение в автоматизированные системы (АС) противника, используемые для обработки интересующей информации;
- подкуп сотрудников из ключевых отделов;
- шантаж и другие способы давления и др.

Несанкционированный доступ к информации, охраняемой как коммерческая тайна квалифицируется, как коммерческий (промышленный) шпионаж. Этот доступ может осуществляется следующими способами:

—хищением носителей информации;

—прослушиванием напрямую или через средства связи разговоров;

—прямого выхода на источник информации с использованием оптических средств;

—перехват сообщений (электронная почта, факс и другие средства);

—через компьютерные сети;

—иным умышленным целенаправленным способом.

Методы сбора информации, обеспечивающие ее добывание, применяются не к собственно информации, а к каналам ее распространения.

Тема 5. Концепция защиты коммерческой тайны

Выделяют следующие **виды защиты информации**:
■ *правовая защита информации*: Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.
■ *техническая защита информации; ТЗИ*: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.
■ *криптографическая защита информации*: Защита информации с помощью ее криптографического преобразования.
■ *физическая защита информации*: Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.
Выделяют *три группы принципов защиты*:
общие принципы защиты,
принципы защиты, касающиеся организационных аспектов,
принципы реализации системы защиты.
К первой группе относят принцип неопределенности; принцип невозможности создания идеальной системы безопасности; принцип минимального риска; принцип минимального ущерба; принцип безопасного времени; принцип защиты от всех.
Ко второй группе относят: принцип законности; принцип персональной ответственности; принцип ограничения полномочий; принцип взаимодействия и сотрудничества;
К третьей группе относят: принцип комплексности и индивидуальности; принцип последовательных рубежей безопасности; принцип равнопрочности и равномощности рубежей безопасности; принцип адекватности и эффективности; принцип секретности; принцип адаптивности; принцип экономичности; принцип эффективности контроля; принцип регистрации; принцип защиты средств обеспечения защиты.

Модель безопасности отображает:
- окружающую среду, содержащую ограничения и угрозы, которые постоянно меняются и известны лишь частично;
- активы организации;

- уязвимости, присущие данным активам;
- меры для защиты активов;
- приемлемые для организации остаточные риски.

Основными компонентами безопасности, вовлеченными в процесс управления, являются:

1. *Активы организации* могут рассматриваться как ценности организации, которые должны иметь гарантированную защиту. Активы включают в себя (но не ограничиваются):
- материальные активы (например вычислительные средства, средства связи, здания);
- информацию (данные) (например документы, базы данных);
- программное обеспечение;
- способность производить продукт или предоставлять услугу;
- людей;
- нематериальные ресурсы (например престиж фирмы, репутацию).

2. *Уязвимость* (vulnerability): Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.

Связанные с активами уязвимости включают в себя слабости физического носителя, организации, процедур, персонала, управления, администрирования, аппаратного/программного обеспечения или информации.

Уязвимость может существовать и в отсутствие угрозы.

Уязвимость сама по себе не причиняет ущерб, но это является только условием или набором условий, позволяющим угрозе воздействовать на активы.

При оценке уровень уязвимости может быть определен как высокий, средний или низкий.

3. Угрозы

Угроза (threat): Потенциальная причина инцидента, который может нанести ущерб системе или организации.

Инцидент информационной безопасности (information security incident)**:** Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Угрозы обладают следующими характеристиками, устанавливающими их взаимосвязь с другими компонентами безопасности:
- источник, внутренний или внешний;
- мотивация, например финансовая выгода, конкурентное преимущество;
- частота возникновения;
- правдоподобие;
- вредоносное воздействие.

При оценке *уровень угрозы* в зависимости от результата ее воздействия может быть определен как высокий, средний или низкий.

4. Воздействие — это результат инцидента информационной безопасности, вызванного угрозой и нанесшего ущерб ее активу.

Результатом воздействия могут стать разрушение конкретного актива, повреждение ИТТ, нарушение их конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности.
Непрямое воздействие может включать в себя финансовые потери, потерю доли рынка или репутации.
Контроль за воздействием позволяет достичь равновесия между предполагаемыми последствиями инцидента и стоимостью защитных мер.
Количественное и качественное измерение воздействия могут быть проведены:
- определением финансовых потерь;
- использованием эмпирической шкалы серьезности воздействия, например от 1 до 10;
- использованием заранее оговоренных уровней (высокий, средний и низкий).
5. *Риск* — это способность конкретной угрозы использовать уязвимости одного или нескольких видов активов для нанесения ущерба организации.
Одна угроза или группа угроз могут использовать одну уязвимость или группу уязвимостей.
Сценарий риска описывает, как определенная угроза или группа угроз могут использовать уязвимость или группу уязвимостей подверженного угрозе актива. Риск характеризуется комбинацией двух факторов: вероятностью возникновения инцидента и его разрушительным воздействием.
Любое изменение активов, угроз, уязвимостей или защитных мер может оказать значительное влияние на риск. Раннее обнаружение или знание обо всех этих изменениях увеличивает возможности по принятию необходимых мер для обработки риска.
Обработка риска включает в себя устранение, снижение, перенос и принятие риска.
Следует учитывать, что риск никогда не устраняется полностью.
Принятие остаточного риска является частью заключения о соответствии уровня безопасности потребностям организации.
Руководство организации должно быть поставлено в известность обо всех остаточных рисках, их опасных последствиях и вероятности возникновения инцидентов.
Решение о принятии риска должно приниматься специалистами, имеющими право принимать решение о допустимости опасных последствий при возникновении инцидента и применении дополнительных мер защиты в случае, если уровень остаточного риска неприемлем.
6. *Защитные меры* — это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов.
Эффективная безопасность обычно требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите активов.

Например, механизмы контроля доступа, применяемые к вычислительным средствам, должны подкрепляться аудитом, определенным порядком действий персонала, его обучением, а также физической защитой. Часть защитных мер может быть обеспечена внешними условиями, свойствами актива или может уже существовать в системе или организации.
Порядок выбора защитных мер очень важен для правильного планирования и реализации программы информационной безопасности.
Защитная мера может выполнять много функций безопасности и, наоборот, одна функция безопасности может потребовать нескольких защитных мер.
Защитные меры могут выполнять одну или несколько из следующих *функций*:
- предотвращение;
- сдерживание;
- обнаружение;
- ограничение;
- исправление;
- восстановление;
- мониторинг;
- осведомление.

Пример — Области, в которых могут использоваться защитные меры, включают в себя:
- физическую среду;
- техническую среду (аппаратно-программное обеспечение и средства связи);
- персонал;
- администрирование.

В процессе выбора защитных мер, предлагаемых для реализации, необходимо учитывать ряд факторов, таких как:
- доступность использования защитных мер;
- прозрачность защитных мер для сотрудников;
- в какой мере использование защитных мер помогает сотрудникам решать свои задачи;
- относительная надежность (стойкость) системы безопасности;
- виды выполняемых функций — предупреждение, сдерживание, обнаружение, восстановление, исправление, мониторинг и обмен информацией.

7. Обычно ограничения устанавливает или признает руководство организации, а также определяет среда, в которой действует организация.
Пример — Такие ограничения могут включать в себя: - организационные;- коммерческие;- финансовые;- по окружающей среде;
- по персоналу;- временные;- правовые;- технические;- культурные/социальные.
Ограничения, присущие организации, должны учитываться при выборе и реализации защитных мер. Необходимо периодически пересматривать существующие и учитывать новые ограничения. Следует отметить, что

ограничения могут со временем изменяться в зависимости от положения организации и изменения внешней среды.

Внешняя среда, в которой действует организация, имеет отношение к нескольким компонентам безопасности, в частности к угрозам, рискам и защитным мерам

Тема 6. Правовое обеспечение сохранности коммерческой тайны на предприятии

Режим коммерческой тайны – правовые, организационные, технические и иные меры, принимаемые в целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну.

Право на установление в отношении сведений режима коммерческой тайны принадлежит лицу, правомерно обладающему такими сведениями.

Режим коммерческой тайны считается установленным после определения состава сведений, подлежащих охране в режиме коммерческой тайны, и принятия лицом, правомерно обладающим такими сведениями, совокупности мер, необходимых для обеспечения их конфиденциальности.

Режим коммерческой тайны включает в себя следующие меры:

■ ограничение доступа к коммерческой тайне путем установления порядка обращения с носителями коммерческой тайны, а также контроля за соблюдением такого порядка;

■ учет лиц, получивших доступ к коммерческой тайне;

■ регулирование отношений, связанных с доступом работников к коммерческой тайне, на основании трудового договора (контракта), а также на основании обязательства о неразглашении коммерческой тайны, дополнительно заключаемого по требованию нанимателя с работником, получающим доступ к коммерческой тайне;

■регулирование отношений, связанных с доступом контрагентов к коммерческой тайне, на основании гражданско-правового договора;

■ определение работников, ответственных за принятие мер по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Владелец коммерческой тайны вправе применять не запрещенные законодательством технические средства и методы защиты информации, а также другие меры, не противоречащие законодательству.

Работник имеет право обжаловать в судебном порядке принятие или изменение нанимателем отдельных мер по обеспечению конфиденциальности сведений, составляющих коммерческую тайну, ограничивающих его права.

Владелец коммерческой тайны может на носителях коммерческой тайны применять гриф «Коммерческая тайна» с указанием владельца коммерческой тайны (для юридических лиц – полное наименование и место нахождения, для физических лиц – фамилия, собственное имя, отчество (если таковое имеется) гражданина и место его жительства).

Владелец коммерческой тайны вправе:

изменять или отменять режим коммерческой тайны;

изменять состав сведений, составляющих коммерческую тайну;

использовать сведения, составляющие коммерческую тайну;

разрешать или запрещать доступ других лиц к коммерческой тайне, изменять порядок и условия доступа к ней, если иное не установлено Законом и иными законодательными актами;

распоряжаться сведениями, составляющими коммерческую тайну;
применять предусмотренные гражданским законодательством способы защиты от действий (бездействия) лиц, нарушающих режим коммерческой тайны или создающих угрозу такого нарушения.
Владелец коммерческой тайны может передать все или часть сведений, составляющих коммерческую тайну, другому лицу по договору, обязательным условием которого является обеспечение конфиденциальности передаваемых сведений.
Владелец коммерческой тайны обязан: поддерживать установленный им режим коммерческой тайны, принимать меры, необходимые и достаточные для обеспечения конфиденциальности сведений, составляющих коммерческую тайну.
Для выполнения этих обязанностей владелец коммерческой тайны вправе:
требовать от лиц, в том числе от государственных органов, получивших доступ к коммерческой тайне, исполнения предусмотренных Законом и (или) договором обязательств по соблюдению конфиденциальности сведений, составляющих коммерческую тайну;
требовать от лиц, получивших возможность ознакомления со сведениями, составляющими коммерческую тайну, в результате случайности либо действий других лиц, которые не имели права предоставлять доступ к коммерческой тайне, соблюдения конфиденциальности этих сведений;
совершать иные действия для обеспечения конфиденциальности сведений, составляющих коммерческую тайну.
В настоящее время за нарушение прав владельца коммерческой тайны законодательством установлены следующие *виды ответственности*:
■ Ответственность в рамках трудовых отношений ;
■ Гражданско-правовая ответственность;
■ Административная ответственность ;
■ Уголовная ответственность.
I. За несоблюдение режима работы с информацией, составляющей коммерческую тайну, к работникам может быть применена материальная и дисциплинарная ответственность.
II. В п.4 ст. 140 ГК обязанность возлагается на работников, разгласивших служебную тайну или коммерческую тайну вопреки обязательству о неразглашении коммерческой тайны, трудовому договору (контракту), и на контрагентов, сделавших это вопреки гражданско-правовому договору.
В случае незаконного ознакомления или незаконного использования, а также разглашения информации, которая составляет служебную тайну или коммерческую тайну, физические и юридические лица, государственные органы и их должностные лица обязаны возместить ее обладателю причиненные убытки.
В соответствии со ст.1011 ГК :
1. Лицо, правомерно обладающее секретом производства (ноу-хау), вправе потребовать от лица, незаконно его использующего, немедленного

прекращения такого использования, а также вправе использовать иные способы защиты, предусмотренные законодательством.
2. В случае использования секрета производства (ноу-хау) лицом, которое в соответствии с законодательством является добросовестным приобретателем, суд с учетом средств, израсходованных таким лицом на использование секрета производства (ноу-хау), может разрешить его дальнейшее использование на условиях возмездности.
3. Лицо, самостоятельно и правомерно получившее сведения, составляющие секрет производства (ноу-хау), вправе использовать эти сведения независимо от прав обладателя соответствующего секрета производства (ноу-хау) и не отвечает перед ним за такое использование.
III. В соответствии со ст.22.13 КоАп умышленное разглашение коммерческой или иной охраняемой законом тайны без согласия ее владельца лицом, которому такая коммерческая или иная тайна известна в связи с его профессиональной или служебной деятельностью, если это деяние не влечет уголовной ответственности, -влечет наложение штрафа в размере от четырех до двадцати базовых величин.
IV Уголовный кодексом предусмотрены следующие преступления, связанные с нарушением требований охраны коммерческой тайны: коммерческий шпионаж (ст.254); разглашение коммерческой тайны (ст.255); незаконное использование либо распространение информации о результатах финансово-хозяйственной деятельности эмитента ценных бумаг (ст.226-1).

Наниматель, являющийся владельцем коммерческой тайны или получивший доступ к коммерческой тайне третьих лиц, обязан:
■ ознакомить работников, которым доступ к коммерческой тайне необходим для выполнения трудовых (служебных) обязанностей, с категориями сведений, составляющих коммерческую тайну нанимателя, и (или) сведений, составляющих коммерческую тайну третьих лиц, к которым наниматель получил доступ (без раскрытия содержания этих сведений);
■ ознакомить работников, получающих доступ к коммерческой тайне, с установленным им режимом коммерческой тайны и мерами ответственности за его нарушение, а также за разглашение сведений, составляющих коммерческую тайну нанимателя, и (или) сведений, составляющих коммерческую тайну третьих лиц, к которым наниматель получил доступ;
■ создать работникам необходимые условия для соблюдения установленного им режима коммерческой тайны.

В целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну, работники обязаны:
■ соблюдать установленный нанимателем режим коммерческой тайны, не разглашать сведения, составляющие коммерческую тайну нанимателя, или сведения, составляющие коммерческую тайну третьих лиц, к которым наниматель получил доступ, и не использовать сведения, составляющие

коммерческую тайну, в целях, не связанных с выполнением трудовых (служебных) обязанностей;
■ подписать по требованию нанимателя обязательство о неразглашении коммерческой тайны;
■ передать нанимателю при прекращении трудового договора (контракта) находящиеся у них носители коммерческой тайны;
■ незамедлительно сообщать нанимателю о допущенных ими либо ставших известными им фактах незаконного ознакомления со сведениями, составляющими коммерческую тайну нанимателя, и (или) сведениями, составляющими коммерческую тайну третьих лиц, к которым наниматель получил доступ, фактах незаконного использования этих сведений, фактах разглашения или угрозы разглашения сведений, составляющих коммерческую тайну нанимателя, и (или) сведений, составляющих коммерческую тайну третьих лиц, к которым наниматель получил доступ, а также о требованиях доступа к коммерческой тайне со стороны государственных органов и иных лиц.
Обязательство о неразглашении коммерческой тайны определяет:
■ права и обязанности сторон, связанные с соблюдением конфиденциальности сведений, составляющих коммерческую тайну,
■ порядок доступа работника к сведениям, составляющим коммерческую тайну нанимателя, и (или) сведениям, составляющим коммерческую тайну третьих лиц, к которым наниматель получил доступ, а также
■ срок действия обязательства.

Обязательство о неразглашении коммерческой тайны:
■ может содержать условие о выплате работнику вознаграждения за выполнение обязательств, связанных с соблюдением режима коммерческой тайны, а также условие об ответственности работника за его нарушение;
■ должно содержать условие об ответственности нанимателя за ненадлежащее выполнение обязанности в письменной форме уведомить контрагентов, работников, в том числе бывших работников, в отношении которых действует обязательство о неразглашении коммерческой тайны, о затрагивающих их права и законные интересы изменении или отмене режима коммерческой тайны в целом либо в отношении отдельных сведений, составляющих коммерческую тайну.

Контрагент – сторона гражданско-правового договора (за исключением лиц, состоящих в трудовых отношениях с владельцем коммерческой тайны), которой владелец коммерческой тайны предоставляет доступ к сведениям, составляющим коммерческую тайну.
Соглашение о конфиденциальности – гражданско-правовой договор, заключаемый владельцем коммерческой тайны с контрагентом, предметом которого являются обязательства сторон по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

До заключения с контрагентом гражданско-правового договора независимо от его вида в целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну и относящихся к предмету заключаемого договора, обязательства по обеспечению конфиденциальности этих сведений могут быть закреплены в самостоятельном соглашении о конфиденциальности.

Обязательства по обеспечению конфиденциальности сведений, составляющих коммерческую тайну, могут быть также предусмотрены самим договором с контрагентом.

Соглашение о конфиденциальности, а также любой иной гражданско-правовой договор с контрагентом, закрепляющий обязательства по обеспечению конфиденциальности сведений, составляющих коммерческую тайну, должны быть оформлены в письменной форме и должны содержать перечень сведений, составляющих коммерческую тайну, или порядок их определения, пределы использования этих сведений, а также указание о сроке, в течение которого контрагент обязан обеспечивать их конфиденциальность, в том числе в случае расторжения или отказа от исполнения договора.

Недействительность гражданско-правового договора с контрагентом не влечет за собой недействительности его части, содержащей обязательства по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Если иное не установлено соглашением сторон, контрагент самостоятельно определяет необходимые способы обеспечения конфиденциальности сведений, составляющих коммерческую тайну, к которым он получил доступ. При этом в отношении третьих лиц контрагент имеет те же права на защиту коммерческой тайны, что и ее владелец, если иное не определено заключенным между ними договором.

Тема 7. Служба безопасности предприятия

В задачи службы безопасности входит определение целей и приоритетных направлений работы по обеспечению безопасности деятельности предприятия.

Составляющие безопасности:

физическая безопасность;

безопасность внешней деятельности;

информационная безопасность;

психологическую безопасность.

Функции СБ по обеспечению *физической безопасности*:

• обнаружение проникновения нарушителя на охраняемую территорию;

• охрана имущества предприятия;

• защита руководителей предприятия;

• обеспечение пропускного режима, разграничение доступа на объект;

• организация инженерно-технической защиты охраняемых зданий, помещений.

Функции по обеспечению *безопасности внешней деятельности:*

• изучение криминальных аспектов рынка;

• противодействие экономическому шпионажу;

• выявление ненадежных деловых партнеров;

• борьба с недобросовестной конкуренцией, в том числе выявление фактов незаконного использования чужой интеллектуальной собственности.

Функции по обеспечению *информационной безопасности*

• организация конфиденциального делопроизводства;

• ограничение круга лиц, работающих с конфиденциальными документами;

• организация ведения конфиденциальных переговоров;

• расследование обстоятельств разглашения сведений, составляющих коммерческую тайну;

• мероприятия по противодействию техническим способам несанкционированного съема информации;

• мероприятия по защите информации, циркулирующей в компьютерах, вычислительных сетях.

Функции по обеспечению *психологической безопасности:*

• выявление неблагонадежных сотрудников;

• профилактические мероприятия по формированию правосознательного поведения сотрудников.

Служба безопасности является исполнительным органом, реализующим решения директора по вопросам безопасности. Служба обеспечивает функциональное управление деятельностью специализированных подразделений, решающих конкретные задачи в сфере безопасности.

Структура службы безопасности определяется ее целями. В составе СБ могут быть созданы информационно-аналитические подразделения,

организационные звенья по направлениям обеспечения безопасности, а также временные структуры для решения конкретных задач.
К организационным мероприятиям защиты информации относятся:
— выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;
— выделение специальных ЭВМ для обработки конфиденциальной информации;
— организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;
— использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;
— организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;
— организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;
— установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;
— разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;
— постоянный контроль за соблюдением установленных требований по защите информации.

Должен быть соблюден ряд условий, выполнение которых свидетельствует о правомерном доступе лица к конфиденциальной информации, а именно:
■ подписание работником обязательства о неразглашении сведений, составляющих коммерческую тайну;
■ наличие у него допуска к таким сведениям и работам;
■ разрешение руководителя структурного подразделения на ознакомление с конкретной конфиденциальной информацией.

Тема 8. Управление персоналом и защита коммерческой тайны

Определение круга лиц, имеющих доступ к коммерческой тайне, предполагает решение следующих задач:

■ выделение конкретных должностей, дающих возможность доступа к ключевой информации,

■ определение критерия добросовестности персонала,

■ подбор персонала с учетом требований безопасности.

Критерий добросовестности работника на практике может рассматриваться с учетом оценки степени важности и ответственности должности, занимаемой работником, участия работника в создании информации, составляющей коммерческую тайну, соответствия его действий требованиям предпринимательской и служебной этики.

Оценке подлежат личностные и профессиональные качества работника, а также его связи. Сбор и систематизация информации может осуществляться, например, путем анкетирования и психологического тестирования [11].

В процессе изучения и оценки персонала не следует забывать и о ряде ограничений, установленных действующим законодательством и направленных в первую очередь на защиту интересов работника. В силу требований их защиты работодатель должен обеспечить:

1) неприкосновенность средств личного общения работника. Существо данного компонента предусматривает, что никто, в том числе работодатель, не может знакомиться с личными письмами, телефонными переговорами работника и средствами визуального воспроизведения, принадлежащими работнику без его согласия;

2) неприкосновенность частной документации работника. По своей юридической природе документация работника может принадлежать либо к деловой (официальной), либо к частной. Различия между этими двумя видами определяются содержанием, характером документации, ее формой и функциональным назначением. Личная же документация не связана какими-либо формальными требованиями (например, не содержит в себе сведений о наличии определенной резолюции должностных лиц работодателя) и содержит информацию о личной жизни работника либо информацию, непосредственно затрагивающую обстоятельства, связанные с личной жизнью;

3) неприкосновенность внешнего облика работника. Работодатель, по общему правилу, не должен определять внешний облик работника во время его присутствия. Нарушение неприкосновенности внешнего облика работника не означает сопряженности данного процесса с каким-либо физическим воздействием. Речь, скорее, идет о психологическом давлении на работника (например, угрозой увольнения со стороны работодателя или понижением суммы заработной платы);

4) неприменение средств специального контроля за достоверностью информации, предоставляемой работником. В данную группу необходимо

законодательно отнести ограничения на использование так называемого детектора лжи, затребования различных справок от третьих лиц о пребывании, например, работника в медицинском вытрезвителе;
5) неприменение средств аудиовизуального контроля за поведением работника на рабочем месте. Указанный компонент означает обеспеченную законом возможность допустимой конфиденциальности действий работника на территории работодателя. Излишне говорить, что и данное право требует определенных ограничений, связанных с обеспечением безопасности производства, сохранностью имущества работодателя и пр.;
6) физическую неприкосновенность работника.
Речь в данном случае должна идти о защите работника, например от необоснованных обысков на территории предприятия, где он работает, от нежелательного внимания со стороны работодателя, выраженного в каких-либо действиях сексуальной направленности и т.п. [14].

В задачи комплексной проверки может входить:
- 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 подозрения о наличии у них каких-либо черт характера, близких к пограничным состояниям;
- фиксирование тех кандидатов, которые не обладают качествами, противопоказанными для принятия на работу, хотя при этом их профессионально значимые качества пока не сформированы либо сформированы, но в недостаточной степени;
- выделение из группы кандидатов тех лиц, которые по своим психологическим характеристикам соответствуют требованиям профессиограмм полностью либо частично.
Как правило, к проблемному персоналу относят:
■ конфликтный персонал;
■ персонал, подверженный воздействию;
■ карьеристы;
■ недовольные (амбициозные);
■ любители красивой жизни и др.
Среди основных мотивов выдачи информации выделяют:
■ алчность,
■ страх за себя и за своих близких,
■ безразличие,
■ тщеславие,
■ счеты с организацией или конкретными лицами.
В этой связи наиболее уязвимыми категориями работников являются те из них, кто обладает следующими свойствами: обладают моральными изъянами или запятнанной репутацией; имеют долги; сильно привязаны к чему-то или к кому-то; по каким либо причинам (например, затруднения в карьерном росте) сильно раздражены.

Существует методики оценки опасности разглашения конфиденциальной информации работниками организации.
Здесь используются вероятностные весовые коэффициенты, величину которых предлагается определять службе безопасности или специально привлекаемыми экспертами.
Суть методики состоит в том, что для каждого сотрудника необходимо определить коэффициенты осведомленности и уязвимости.
Коэффициент осведомленности присваивается в зависимости от того, насколько данный сотрудник по своему служебному положению имеет доступ к информации, утечка которой может нанести вред предприятию. Численное значение этого коэффициента должно располагаться в пределах от 0 до 1.
Если, к примеру, сотрудник осведомлен слабо, коэффициент не будет превышать значений 0,1–0,2; если в средней степени, то в пределах 0,4–0,5. Коэффициент значением более 0,8 означает высокую степень осведомленности. Значения коэффициентов должны выбираться с учетом хорошего знания участка работы и личных качеств сотрудника.
Коэффициент уязвимости выбирается в тех же числовых пределах, исходя из:
- служебного положения сотрудника;
- опасности, которую представляет утечка известной сотруднику информации;
- степени известности окружению о том, в чем сотрудник осведомлен;
- степени удовлетворенности работником своим положением и его моральных качеств.

Произведение этих двух коэффициентов будет определять вероятностную характеристику угрозы.
Если результирующая величина получилась менее 0,1, можно не принимать никаких специальных мер.
Если эта цифра достигает величины 0,4–0,5, то данный сотрудник должен быть в зоне внимания службы безопасности, о нем должна накапливаться информация и регулярно пересматриваться значение его коэффициентов.
Превышение величины вероятности угрозы свыше 0,8 должно быть сигналом к принятию специальных мер защиты сотрудника.
Такой подход является в определенной мере приблизительным, но по мере накопления опыта оценки он может давать неплохие результаты.

Цель программы обеспечения компетентности в вопросах безопасности состоит в том, чтобы повысить знания сотрудников организации до необходимого уровня, когда процессы обеспечения безопасности становятся регулярными и все сотрудники их выполняют.
Эффективными можно считать только те меры защиты, которые хорошо усвоены персоналом организации и конечными пользователями.
Данные для программы обеспечения компетентности в вопросах безопасности должны поступать от всех подразделений организации.
Рекомендуется включать в список следующие темы:

- определение понятия «безопасность»;
- предупреждение нарушений конфиденциальности, целостности и доступности;
- потенциальные угрозы, которые могут оказать неблагоприятное воздействие на производственную деятельность организации и сотрудников;
- классификация чувствительности информации;
- процесс обеспечения общей безопасности;
- описание процесса обеспечения общей безопасности;
- компоненты анализа риска;
- меры защиты и обучение приемам их применения;
- роли и обязанности сотрудников;
- политика информационной безопасности.

Функция	HR	СББ
Наем персонала	Проверка кандидатов на профессиональную пригодность и квалифицированность	Проверка кандидатов на криминогенность, потенциальную лояльность и выяснение истинных причин устройства на работу
Адаптация персонала	Адаптация нового персонала в коллективе и изучение всех особенностей организации	Установление доверительных отношений в целях получения объективной информации
Обучение персонала	Исходное обучение персонала, плановое повышение его квалификации и организация переподготовки работников в рамках профессии и занимаемой должности	Исходное обучение персонала, плановое повышение его квалификации и проведение переподготовки работников в рамках комплексной системы безопасности организации
Управление персоналом	Управление персоналом в целях достижения максимальной эффективности его работы (в рамках занимаемой должности)	Управление персоналом в целях снижения внутренних угроз, связанных с сотрудниками организации
Лояльность и мотивированность персонала	Создание и поддержание высокого уровня лояльности и мотивированности персонала в целях снижения текучки кадров и повышения эффективности работы	Поддержание высокого уровня лояльности и мотивированности персонала в целях снижения внутренних угроз, связанных с сотрудниками организации
«Безопасное» увольнение персонала	Создание положительной мотивации по отношению к организации у увольняемых сотрудников	Создание положительной мотивации по отношению к организации у увольняемых сотрудников

Алгоритм кадровых действий при увольнении по п. 6 ст. 47 ТК
Шаг 1. Оформление факта разглашения коммерческой тайны.
Шаг 2. При необходимости создание комиссии по расследованию факта
Шаг 3. Проведение служебного расследования.
Шаг 4. Оформление решения комиссии по расследованию факта разглашения коммерческой тайны работником, имеющим к ней доступ (при условии ее создания).
Шаг 5. Проверка наличия всех необходимых условий для увольнения работника по п. 6 ст. 47 ТК (разглашение коммерческой тайны работником, имеющим к ней доступ).
Шаг 6. Оформление приказа об увольнении по п. 6 ст. 47 ТК.
Шаг 7. Включение копии приказа об увольнении в личное дело работника (если оно ведется в соответствии с законодательством о делопроизводстве).
Шаг 8. Внесение записи в трудовую книжку.
Шаг 9. Оформление личной карточки при прекращении трудового договора.
Шаг 10. В последний день работы выдача работнику трудовой книжки и произведение с ним окончательного расчета.

Шаг 11. Сдача личного дела (если оно было оформлено согласно требованиям законодательства) в архив.
Шаг 12. Направление в военкомат сведений об уволенном работнике, подлежащему воинскому учету.
Шаг 13. Оформление документов по персонифицированному учету (ПУ-2) и представление их в территориальные органы Фонда социальной защиты населения Министерства труда и социальной защиты Республики Беларусь.

Условия увольнения по п. 6 ст. 47 ТК
1) работнику для исполнения своих трудовых обязанностей необходим доступ к коммерческой тайне;
2) у нанимателя установлен режим коммерческой тайны;
3) нанимателем были созданы условия для соблюдения установленного режима коммерческой тайны;
4) работник ознакомлен с обязанностью соблюдать режим коммерческой тайны;
5) коммерческая тайна стала или должна была стать известной работнику в связи с исполнением трудовых обязанностей;
6) наличие доказательств разглашения работником коммерческой тайны.