Организационное и правовое обеспечение информационной безопасности.

«Подбор и работа с кадрами в сфере информационной безопасности. Кадровая безопасность»

Выполнила:
Студентка группы з-76Б
Лукьяненко М.В.

Кадровая безопасность- это процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом.

Вся деятельность служб персонала может быть разложена на этапы (поиск, отбор, прием, адаптация и т.д. вплоть до увольнения и далее).
Любое действие менеджера по персоналу на любом этапе — это либо усиление, либо ослабление безопасности компании по главной ее составляющей — по кадрам.

Около 80% ущерба материальным активам компаний наносится их собственным персоналом. Только 20% попыток взлома сетей и получения несанкционированного доступа к компьютерной информации приходит извне.

В определении понятия кадровой безопасности было отмечено, что это процесс предотвращения угроз. Они представляют из себя негативные воздействия, отрицательно влияющие на состояние кадровой функциональной составляющей экономической безопасности предприятия. Проще говоря, безопасность — это предотвращение убытков. Для этого необходимо проводить постоянную работу по предотвра и убытки.

Следует различать внешние и внутренние угрозы. Внешние негативные воздействия — это действия, явления или процессы, не зависящие от воли и сознания работников предприятия и влекущие нанесение ущерба. В свою очередь, к внутренним негативным воздействиям относятся действия (умышленные или неосторожные) сотрудников предприятия, также влекущие нанесение ущерба.

Например, внутренние опасности таковы:
• несоответствие квалификации сотрудников предъявляемым к ним требованиям;
• недостаточная квалификация сотрудников;
• слабая организация системы управления персоналом;
• слабая организация системы обучения;
• неэффективная система мотивации;

Понятия

1. Безопасность организации - это такое состояние, которое достигается посредством обеспечения и поддержания защищенности ее персонала и жизненно важных интересов организации от внутренних и внешних угроз с целью уменьшения отрицательных последствий нежелательных событий и достижения наилучших результатов деятельности.
2. Угроза безопасности организации - это событие, действие или явление, которое посредством воздействия на персонал, финансовые, материальные ценности и информацию может привести к нанесению вреда здоровью работников и ущерба организации, нарушению или приостановке ее функционирования.
3. Обеспечение безопасности организации - это деятельность ее должностных лиц, персонала, специального подразделения по безопасности, государственных правоохранительных органов и иных структур, направленная на предотвращение возможного нарушения ее нормального функционирования.
4. Система безопасности организации - это комплекс организационно - управленческих, экономических, правовых, социально-психологических, профилактических, пропагандистских, режимных и инженерно-технических мер и мероприятий, направленных на обеспечение безопасности организации и ее персонала.

Обеспечение безопасности организации должно соответствовать следующим принципам:

- непрерывность
- комплексность
- своевременность
- законность
- активность
- универсальность
- экономическая целесообразность
- конкретность и надежность
- профессионализм
- взаимодействие и координация
- централизация управления и автономнос

Основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы в области защиты информации:

1. Конституция РФ;
2. Закон Российской Федерации от 21.07.1993 N 5485-1 «О государственной тайне»;
3. Вопросам защиты персональных данных посвящена специальная глава Трудового кодекса РФ (глава 14 — «Защита персональных данных работника»), а также Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
4. В ст. 11 Федерального закона от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (в редакции от 11.07.2011) урегулирован вопрос конфиденциальности информации в рамках трудовых отношений; его положения обязательно учитываются при оформлении на должность, предполагающую работу с конфиденциальной информацией, в том числе с персональными данными и

Методические нормативные акты:

Каждая служба кадров в своей деятельности руководствуется, помимо законодательных актов, также методическими нормативными документами, регламентирующими процедуру выполнения отдельных действий (операций, записей и т. п.).

1 Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895

2 Положение о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 27 октября 1995 г. № 199 и т.д.

Система безопасности обеспечивается работой таких подразделений, как:

Компьютерная безопасность. Работа этого подразделения основана на принятии технологических и административных мер, которые обеспечивают качественную работу всех аппаратных компьютерных систем, что позволяет создать единый, целостный, доступный и конфиденциальный ресурс.

Безопасность данных - это защита информации от халатных, случайных, неавторизированных или умышленных разглашений данных или взлома системы.

Безопасное программное обеспечение - это целый комплекс прикладных и общецелевых программных средств, направленных на обеспечение безопасной работы всех систем и безопасную обработку данных.

Безопасность коммуникаций обеспечивается за счет аутентификации систем телекоммуникаций, предотвращающих доступность информации

Обеспечение информационной безопасности организации базируется на принятии таких мер, как:

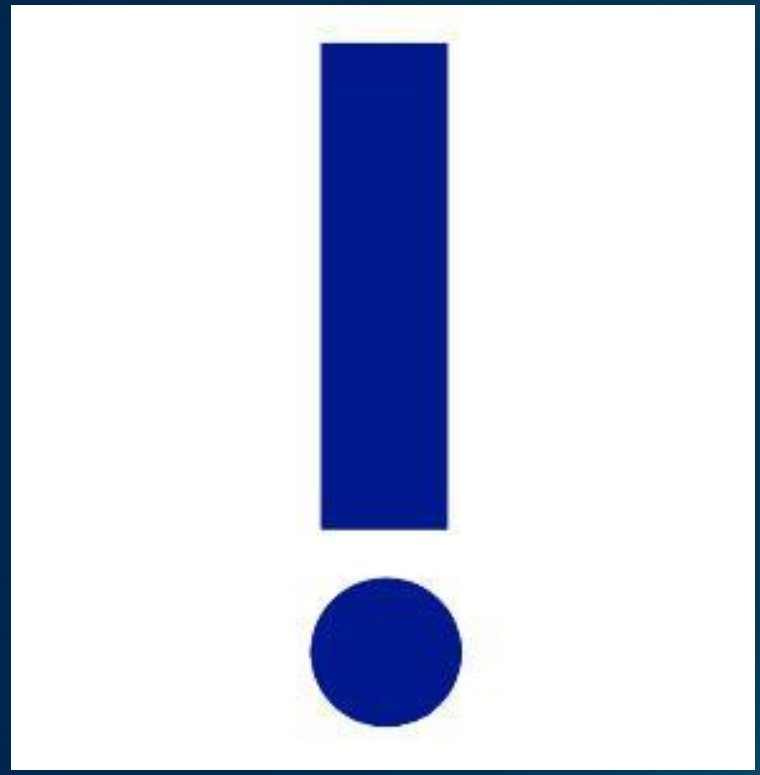
- Анализ потенциальных и реальных ситуаций, представляющих угрозу безопасности информации предприятия;
- Оценка характера угроз безопасности информации;
- Принятие и комплексное распределение мер для определения угрозы;
- Реализация принятых мер по предотвращению угрозы.

Основная цель обеспечения комплексной системы безопасности информации для защиты предприятия, это:

- Создать благоприятные условия для нормального функционирования в условиях нестабильной среды;
- Обеспечить защиту собственной безопасности;
- Возможность на законную защиту собственных интересов от противоправных действий конкурентов;
- Обеспечить сотруднику сохранностью жизни и здоровья.

Для эффективной безопасности нужно:

1. Все используемые средства для защиты должны быть доступными для пользователей и простыми для технического обслуживания.
2. Каждого пользователя нужно обеспечить минимальными привилегиями, необходимыми для выполнения конкретной работы.
3. Система защиты должна быть автономной.
4. Необходимо предусмотреть возможность отключения защитных механизмов в ситуациях, когда они являются помехой для выполнения работ.
5. Разработчики системы безопасности должны учитывать максимальную степень враждебности окружения, то есть предполагать самые наихудшие намерения со стороны злоумышленников и возможность обойти все защитные механизмы.
6. Наличие и место расположение



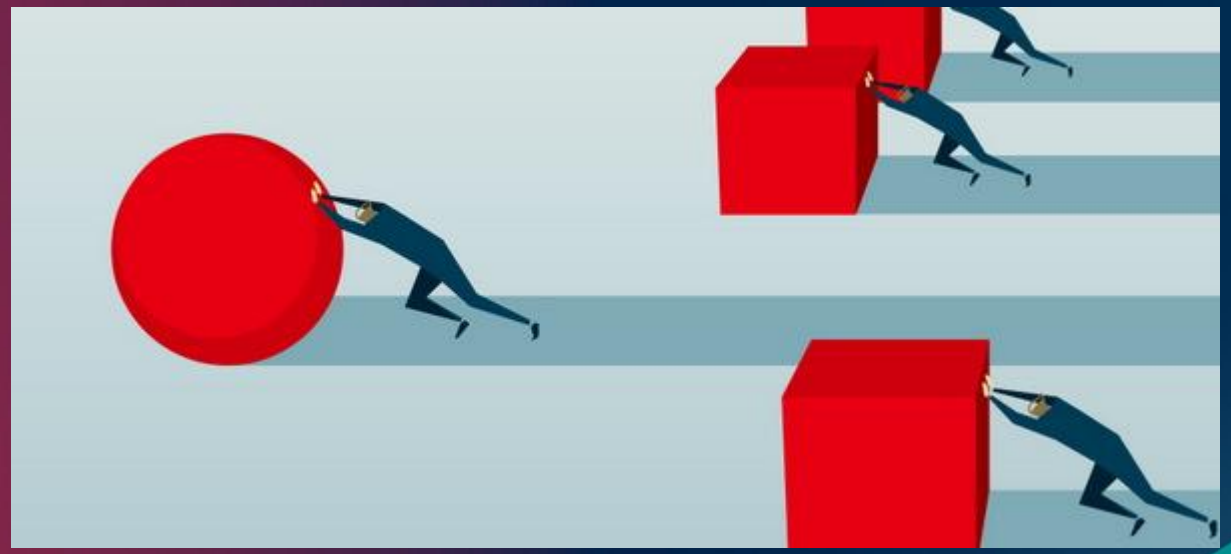
Для обеспечения защиты информации используются следующие методы:

1) Препятствие. Метод представляет собой использование физической силы с целью защиты информации от преступных действий злоумышленников с помощью запрета на доступ к информационным носителям и аппаратуре.

2) Управление доступом – метод, который основан на использовании регулирующих ресурсов автоматизированной системы, предотвращающих доступ к информационным носителям. Управление доступом осуществляется с помощью таких функций, как:

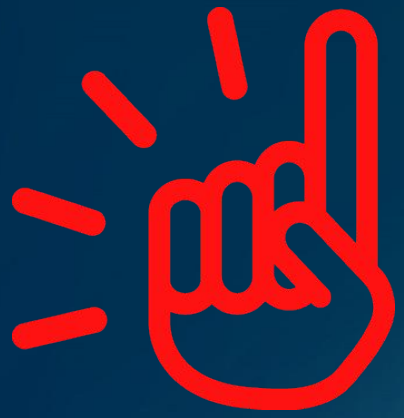
• Идентификация личности пользователя, работающего персонала и систем информационных ресурсов такими мерами, как присвоение каждому пользователю и объекту личного идентификатора;

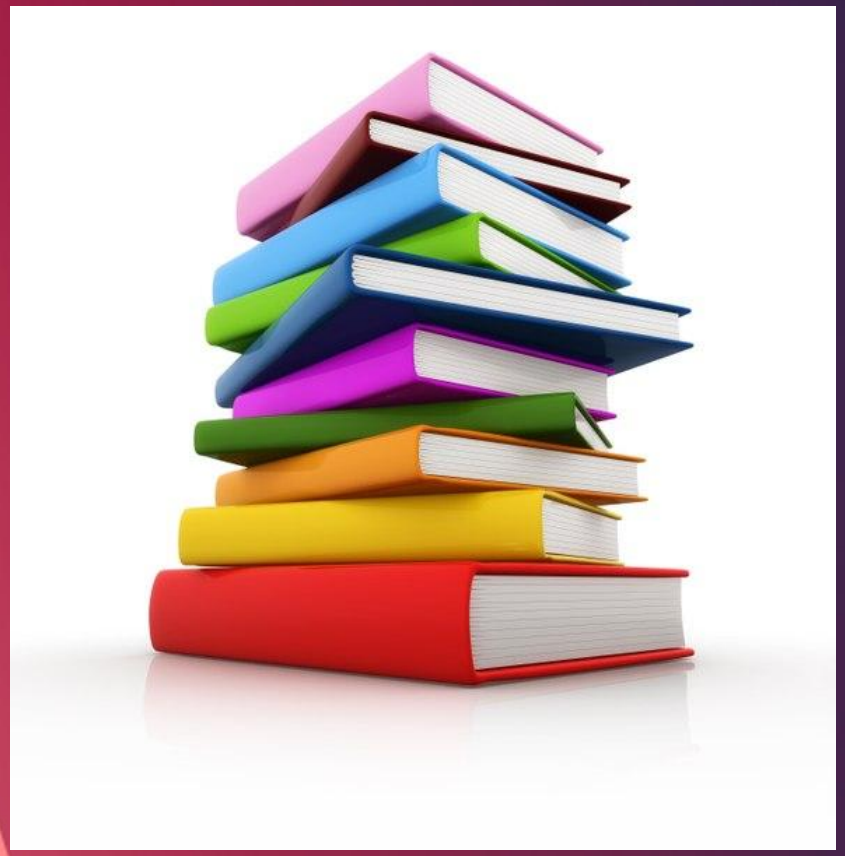
• Аутентификация, которая устанавливает принадлежность субъекта или объекта к заявленному им идентификатору и тд.



3) Маскировка – метод криптографического закрытия, защищающий доступ к информации в автоматизированной системе.
4) Регламентация – метод информационной защиты, при котором доступ к хранению и передаче данных при несанкционированном запросе сводится к минимуму.
5) Принуждение – это метод, который вынуждает пользователей при доступе к закрытой информации соблюдать определенные правила. Нарушение установленного протокола приводит к штрафным санкциям, административной и уголовной ответственности.
6) Побуждение – метод, который основан на этических и моральных нормах, накладывающих запрет на использование запрещенной информации, и побуждает соблюдать установленные правила.

Взаимодействие служб управления персонала и безопасности создаст безопасные условия для эффективной работы организации и обеспечит как личную безопасность работников, так и безопасность организации в целом.
Задача службы управления персоналом и службы безопасности организации





Используемая литература

• Бадалова А. Г., Москвитин К. П. Управление кадровыми рисками предприятия // Российское предпринимательство. 2005. N 7.

• Управление персоналом организации: Учеб. / Под ред. А. Я. Кибанова. М.: ИНФРА-М, 2006.

• https://studme.org/1686111426191/menedzhment/kadrovaya_bezopasnost_organizatsii

• https://www.top-personal.ru/officeworkissue.html?282

• Березюк, Л.П. Организационное обеспечение информационной безопасности : учеб. пособие / Л.П. Березюк. – Хабаровск : Изд-во ДВГУПС,2008. – 188 с.

Лукьяненко Мария Витальевна.
Тел. +7-952-801-33-92
Email: marysa1998@sibmail.com