Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

Организационное и правовое обеспечение

информационной безопасности.

Реферат на тему:

«Подбор и работа с кадрами в сфере информационной безопасности.

Кадровая безопасность.»

Выполнила:

Студентка группы з-76Б

 \_\_\_\_\_/Лукьяненко М.В.

Принял:

Старший преподаватель кафедры КИБЭВС

\_\_\_\_\_\_\_/ Гуляев А.И.

«\_\_»\_\_\_\_\_\_\_\_\_\_\_2019г.

Томск-2019.

Оглавление.

Введение…………………………………………………………..….3

Основная часть……………………………………………….………4

 Понятия……………………………………………………….5

 Принципы для обеспечения безопасности организации…..7

 Нормативные правовые акты…………………………….….9

 Методические нормативные акты…………………………..10

 Система безопасности……………………………………….11

Заключение………………………………………………….………..15

Используемая литература……………………………………………16

Введение

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.

Невооруженным взглядом видно, что кадровая безопасность занимает доминирующее положение по отношению к другим элементам системы безопасности компании, так как она «работает» с персоналом, кадрами, а они в любой составляющей первичны. Таким образом, служба персонала — более важный субъект в кадровой безопасности, чем служба безопасности.

Вся деятельность служб персонала может быть разложена на этапы (поиск, отбор, прием, адаптация и т.д. вплоть до увольнения и далее), и на каждом этапе присутствует масса вопросов безопасности, решаемых именно «персональщиками». 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. Остальные 80% случаев спровоцированы с участием персонала компаний.

Основная часть

В определении понятия кадровой безопасности было отмечено, что это процесс предотвращения угроз. О каких угрозах идет речь? 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 предотвращению угроз, вызывающих эти 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.

Обратив внимание на небольшой список профильных угроз, еще раз убедимся в том, что обеспечение кадровой безопасности является важнейшей составляющей работы менеджера (директора) по персоналу. 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;
* ошибки в планировании ресурсов персонала;
* снижение количества рационализаторских предложений и инициатив;
* уход квалифицированных сотрудников;
* сотрудники ориентированы на решение внутренних тактических задач;
* сотрудники ориентированы на соблюдение интересов подразделения;
* отсутствие или «слабая» корпоративная политика;
* некачественные проверки кандидатов при приеме на работу.

Бесспорно, все эти негативные воздействия внешней среды оказывают влияние на процессы внутри предприятия, в целом, на его безопасность по кадровой составляющей. Кадровая безопасность, являясь элементом экономической безопасности компании, нацелена на такую работу с персоналом, на установление таких трудовых и этических отношений, которые можно было бы определить, как «безубыточные».

 *Понятия, связанные с данной темой:*

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. Определяющим и изначальным при формировании системы безопасности является концепция безопасности организации, которая представляет собой свод основных документов, касающихся политики и стратегии безопасности, основных направлений, средств и методов ее обеспечения.
5. Физическая безопасность объекта - это охрана материальных и финансовых ресурсов от чрезвычайных обстоятельств (пожар, стихийное бедствие, терроризм) и от несанкционированного проникновения на территорию (вандализм, кража, хищение и т. д.). Обеспечение безопасности объектов **регулируется Законом РФ от 11.03.1992 N 2487-1 "О частной детективной и охранной деятельности в Российской Федерации"** (ред. от 27.12.2009), положениями и инструкциями, разрабатываемыми и вводимыми в действие Службой государственного пожарного надзора и Управления вневедомственной охраны МВД России. Этот вид безопасности объекта обеспечивается деятельностью сотрудников службы охраны путем соблюдения пропускного объектового и внутри-объектового режимов с применением соответствующих охранных технических средств и систем.
6. Физическая безопасность персонала - это система охраны труда и техники безопасности в организации на основе производственной санитарии и психологии деловых отношений. Безопасные и здоровые условия труда в организации обеспечиваются комплексным взаимодействием как руководства организации, так и, не в последнюю очередь, усилиями самого персонала организации. Системы охраны труда и техники безопасности в организации **регламентируются Трудовым кодексом РФ (разд. X), Законом РФ "Об основах охраны труда в Российской Федерации"** и нормативными правовыми актами по охране труда.
7. Экономическая безопасность - это состояние защищенности экономических интересов организации от внутренних и внешних угроз посредством минимизации коммерческих рисков, системы мер экономического, правового и организационного характера, разработанной администрацией организации. Экономическая безопасность характеризуется совокупностью качественных и количественных показателей и включает в себя следующие функциональные составляющие: финансовую, имущественную, валютную, кредитную, политико-правовую и др. Экономическая безопасность выступает материальной основой решения практически всех задач, связанных с функционированием организации.
8. Информационная безопасность - это охрана каналов поступления, хранения, обработки и передачи информации, защита любых информационных ресурсов по уровням доступа. Защите подлежит любая документационная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты информации устанавливается в отношении конфиденциальной документационной информации собственником информационных ресурсов, т. е. самой организацией.

Как показывает практический опыт, обеспечение безопасности организации должно соответствовать следующим принципам:

- *непрерывность* - осуществление мер по обеспечению безопасности должно быть основано на постоянной готовности к отражению как внутренних, так и внешних угроз безопасности организации. При этом руководители организаций должны ясно осознавать: процесс обеспечения безопасности не допускает перерывов, иначе придется все начинать сначала;

- *комплексность* - использование всех средств защиты финансовых, материальных, информационных и человеческих ресурсов во всех структурных подразделениях организации и на всех этапах ее деятельности. При этом комплексность реализуется через совокупность правовых, организационных и инженерно-технических мероприятий без их приоритетного выделения;

- *своевременность* - обеспечение безопасности с использованием упреждающих мер. При этом принцип своевременности предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности, а также разработку эффективных мер предупреждения посягательств на интересы организации;

- *законность* - обеспечение безопасности на основе законодательства РФ и других нормативных актов, утвержденных органами государственного управления в пределах их компетенции. При этом необходимо иметь в виду, что вопрос дозволенности тех или иных методов обнаружения и пресечения правонарушений в рамках действующего законодательства и большого количества ведомственных подзаконных актов в настоящее время в большинстве случаев остается открытым;

- *активность* - обеспечение безопасности организации с достаточной степенью настойчивости и с широким использованием маневра имеющихся сил и средств;

- *универсальность* - обеспечение безопасности посредством применения таких мер и проведения таких мероприятий, которые дают положительный эффект независимо от места их конкретного применения;

- *экономическая* *целесообразность* - сопоставление возможного ущерба и затрат на обеспечение безопасности. При этом во всех случаях стоимость системы безопасности должна не превышать размера возможного ущерба от любых видов риска;

- *конкретность* *и* *надежность* - определение конкретных видов ресурсов, выделяемых на обеспечение безопасности. При этом обязательным является достаточное дублирование методов, средств и форм защиты при обеспечении безопасности организации;

- *профессионализм* - реализация мер безопасности должна осуществляться только профессионально подготовленными специалистами. При этом в условиях быстрого развития средств и систем безопасности необходимо постоянное совершенствование мер и средств защиты на базе обучения личного состава;

- *взаимодействие* *и* *координация* - осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений, служб и ответственных лиц. При этом вопрос о взаимодействии и координации касается не только подразделений и лиц, непосредственно отвечающих за безопасность, но и их связи с остальными подразделениями организации;

*- централизация управления и автономность* - обеспечение организационно-функциональной самостоятельности процесса организации защиты всех объектов охраны и централизованное управление обеспечением безопасности организации в целом.

Тесно связана с кадровой безопасностью безопасность труда и здоровья персонала - *система обеспечения безопасности жизни и здоровья работников* в процессе трудовой деятельности, включающая правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия **(ст. 1 Основ законодательства РФ об охране труда).**

*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;
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» N 149-ФЗ от 27.07.2006 (последняя редакция от 29.12.2013) определяет важные для любого кадровика, использующего информационные технологии в работе с кадровыми документами;
6. Закон Российской Федерации от 5 марта 1992 г. № 2446-1 "О безопасности";
7. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 "О сертификации средств защиты информации";
8. Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 " Об организации лицензирования отдельных видов деятельности".

*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. Правила ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденные Постановлением Правительства Российской Федерации от 16.04.2003 N 225 «О трудовых книжках»;
2. Инструкция по заполнению трудовых книжек, утвержденная Постановлением Минтруда России от 10.10.2003 N 69.
3. ГОСТ Р 6.30-2003 закрепляет общие правила составления и оформления документов в унифицированной системе организационно-распорядительной документации с требованиями к оформлению документов;
4. Вопросы хранения, комплектования, учета и использования архивных документов регламентированы Федеральным законом от 22.10.2004 N 125-ФЗ «Об архивном деле в Российской Федерации», а также «Основными правилами работы архивов организаций»;
5. Служба кадров акционерного общества должна также иметь Положение о порядке и сроках хранения документов акционерных обществ, утвержденное Постановлением Федеральной комиссии по рынку ценных бумаг от 16.07.2003 N 03-33/пс (в соответствии со ст. 89 Федерального закона от 26.12.1995 N 208-ФЗ «Об акционерных обществах»);
6. Существует большое количество нормативных документов, содержащих нормы времени на работы, выполняемые сотрудниками управленческого аппарата, разработанных Центральным бюро нормативов по труду (Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления, утв. Постановлением Министерства труда Российской Федерации от 25.11.1994 N 72; Межотраслевые укрупненные нормативы времени на работы по комплектованию и учету кадров. М., 1991; и др.);
7. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895
8. Положение о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 27 октября 1995 г. № 199.

*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 неавторизированным лицам, которая может быть выдана на телекоммуникационный запрос.

Система безопасности потенциальных и реальных угроз непостоянна, поскольку те могут появляться, исчезать, уменьшаться или нарастать. Все участники отношений в процессе обеспечения безопасности информации, будь то человек, государство, предприятие или регион, представляют собой многоцелевые сложные системы, для которых трудно определить уровень необходимой безопасности. На основании этого система обеспечения информационной безопасности организации рассматривается как целый комплекс принятых управленческих решений, направленных на выявление и предотвращение внешних и внутренних угроз. Эффективность принятых мер основывается на определении таких факторов, как степень и характер угрозы, аналитическая оценка кризисной ситуации и рассматривание других неблагоприятных моментов, представляющих опасность для развития предприятия и достижения поставленных целей. 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.

Предотвращать возможность материального и финансового хищения, искажения, разглашения и утечки конфиденциальной информации, растраты, производственные нарушения, уничтожение имущества и обеспечить нормальную производственную деятельность.

Качественная безопасность информации для специалистов - это система мер, которая обеспечивает:

* Защиту от противоправных действий;
* Соблюдение законов во избежание правового наказания и наложения санкций;
* Защиту от криминальных действий конкурентов;
* Защиту от недобросовестности сотрудников.
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 защитных механизмов должно быть конфиденциальной информацией

*5 принципов системы обеспечения информационной безопасности организации*

**Принцип комплексности**. При создании защитных систем необходимо предполагать вероятность возникновения всех возможных угроз для каждой организации, включая каналы закрытого доступа и используемые для них средства защиты. Применение средств защиты должно совпадать с вероятными видами угроз и функционировать как комплексная система защиты, технически дополняя друг друга. Комплексные методы и средства обеспечения информационной безопасности организации являются сложной системой взаимосвязанных между собой процессов.

**Принцип эшелонирования** представляет собой порядок обеспечения информационной безопасности организации, при котором все рубежи защитной системы будут состоять из последовательно расположенных зон безопасности, самая важная из которых будет находиться внутри всей системы.

**Принцип надежности (равнопрочности).** Стандарт организации обеспечения информационной безопасности должен касаться всех зон безопасности. Все они должны быть равнопрочными, то есть иметь одинаковую степень надежной защиты с вероятностью реальной угрозы.

**Принцип разумной достаточности** предполагает разумное применение защитных средств с приемлемым уровнем безопасности без фанатизма создания абсолютной защиты. Обеспечение организации высокоэффективной защитной системой предполагает большие материальные затраты, поэтому к выбору систем безопасности нужно подходить рационально. Стоимость защитной системы не должна превышать размер возможного ущерба и затраты на ее функционирование и обслуживание.

**Принцип непрерывности.** Работа всех систем безопасности должна быть круглосуточной и непрерывной.

*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;
* Проверка соответствия полномочий, которая заключается в установлении точного времени суток, дня недели и ресурсов для проведения запланированных регламентом процедур;
* Доступ для проведения работ установленных регламентом и создание необходимых условий для их проведения;
* Регистрация в виде письменного протоколирования обращений к доступу защитных ресурсов;
* Реагирование на попытку несанкционированных действий в виде шумовой сигнализации, отключения, отказа в запросе и в задержке работ.

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.

Заключение

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 состоит в обеспечении отсутствия опасности.

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.