Министерство образования и науки Челябинской области

Государственное бюджетное профессиональное образовательное учреждение

**«Южно-Уральский государственный технический колледж»**

**методические рекомендации**

**по практическим работам**

по МДК.03.02

**«Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи»**

для специальности 11.02.15

«**Инфокоммуникационные сети и системы связи»**

2020 г.

|  |  |  |
| --- | --- | --- |
| Методические рекомендации составлены в соответствии с утвержденной программой | ОДОБРЕНО  Предметной (цикловой)  комиссией  протокол № 3  от «23» октября 2021 г.  Председатель ПЦК  Михайленко Ю.Н. | УТВЕРЖДАЮ  Заместитель директора  по НМР  \_\_\_\_\_\_\_\_Т.Ю.Крашакова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_2021 г. |

**Составитель:**

Воителева Т.П., преподаватель Южно-Уральского государственного технического колледжа.

Содержание

|  |  |
| --- | --- |
| Введение………………………………………………………………………….. | 2 |
| Практическая работа № 1………………………………………………………  «Выявление потенциально возможных угроз и каналов утечки информации» | 5 |
| Практическая работа № 2………………………………………………………  «Определение состава защищаемой информации» | 13 |
| Практическая работа № 3………………………………………………………  «Определение каналов НСД к информации» | 16 |
| Практическая работа № 4………………………………………………………  «Разработка этапов КСЗИ» | 19 |
| Практическая работа № 5………………………………………………………  «Подбор состава КСЗИ» | 26 |
| Практическая работа № 6 ………………………………………………………  «Защита корпоративной почты» | 32 |
| Практическая работа № 7 ………………………………………………………  «Определение обязанностей конечных пользователей» | 35 |
| Практическая работа № 8………………………………………………………  «Определение ошибок кадрового обеспечения КСЗИ» | 45 |
| Практическая работа № 9………………………………………………………  «Разработка кодекса корпоративного поведения» | 54 |
| Практическая работа № 10………………………………………………………  «Выявление проблем ЗИ на предприятии и определение механизмов КСЗИ» | 62 |
| Практическая работа № 11………………………………………………………  «Определение возможных чрезвычайных ситуаций на предприятии» | 63 |
| Практическая работа № 12………………………………………………………  «Составление перечня информации для проведения аудита ИБ» | 69 |
| Практическая работа № 13………………………………………………………  «Составление инструкции при работе с ПК для сотрудников организации» | 71 |
| Практическая работа № 14………………………………………………………  «Разработка инструкции по составлению пароля» | 73 |
| Практическая работа № 15………………………………………………………  «Составление перечня нормативно-методического обеспечения ИБ» | 75 |
| Список литературы…………………………………………………………….. | 80 |

Введение

Для овладения знаниями и их закрепления, приобретения умений и навыков, необходимых в дальнейшей познавательной и трудовой деятельности и служащих основой рационализаторской, исследовательской и управленческой деятельности, необходимы практические занятия. Практические работы относятся к основным видам учебных занятий.

Практические работы в курсе изучения МДК.02.02."Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи" способствуют овладению указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями:

* ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности;
* ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
* ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.

Обучающийся в ходе выполнения практических работ должен:

знать:

* принципы построения информационно-коммуникационных сетей;
* международные стандарты информационной безопасности;
* акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;
* технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
* классификацию угроз сетевой безопасности;
* методы и способы защиты информации, передаваемой по кабельным направляющим системам;
* правила проведения возможных проверок согласно нормативным документам Федеральной службы по техническому и экспортному контролю;
* средства защиты различных операционных систем и среды передачи информации.

уметь:

* классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
* определять оптимальные способы обеспечения информационной безопасности;
* осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
* выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
* выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
* защищать базы данных при помощи специализированных программных продуктов.

Ведущими целями проведения практических занятий являются:

* обобщение, систематизация, углубление, закрепление полученных теоретических знаний по дисциплине;
* формирование умений применять полученные знания на практике;
* развитие интеллектуальных умений: аналитических, проектировочных, конструкторских;
* выработка таких профессионально значимых качеств, как самостоятельность, ответственность, творческая инициатива, умение работать в коллективе.

Выполнение каждой работы предваряет краткий теоретический материал, необходимый для усвоения данной темы. До начала выполнения студенты должны ознакомиться с целью работы, теорией по данной теме, порядком выполнения работы.

По результатам выполненной практической работы студенты должны оформить отчет, и ответить на контрольные вопросы.

Практическая работа № 1

«Выявление потенциально возможных угроз и каналов утечки информации»

**Цель**. Получение практических навыков выявления потенциально возможных угроз и каналов утечки информации.

1. Общие положения

Чтобы дать исчерпывающую характеристику реального состояния объекта информационной безопасности в конкретный момент времени, необходимо описать не только сущность, виды и основы формирования угроз его информационной безопасности, но и возможные каналы утечки конфиденциальной информации.

В первую очередь необходимо рассмотреть основные понятия и некоторые основополагающие принципы теории информации.

Источник информации — объект, осуществляющий выбор из всей совокупности информационных сообщений одного сообщения, подлежащего передаче по каналу связи адресату. В нашем случае источником информации может быть сотрудник предприятия, в установленном порядке допущенный к конфиденциальной информации, работающий с документами или иными ее носителями. В процессе разработки (формирования) документа осуществляется преобразование информации в форму сообщения.

Сообщение — набор знаков (текст документа), с помощью которых сведения могут быть переданы другому объекту и восприняты им. В отдельных случаях в целях исключения (существенного уменьшения) вероятности овладения посторонним лицом (злоумышленником) охраняемой информацией преобразование информации в текст документа осуществляется с использованием криптографических или программно-аппаратных средств защиты.

Отправитель сообщения — объект, осуществляющий непосредственную передачу документа, содержащего конфиденциальную информацию, адресату. В роли отправителя документа может выступать сотрудник режимно-секретного подразделения (службы безопасности) предприятия, осуществляющий непосредственную отправку (доставку) документа по назначению (в соответствии с указанным адресом). Также отправителем может быть оператор (сотрудник структурного подразделения), осуществляющий передачу документа с использованием технических средств передачи и обработки информации (технических средств связи).

Передатчик — устройство, выполняющее функцию обработки сообщения в соответствии с выбранным алгоритмом и формирования сигнала для непосредственной его передачи по каналу связи (информационному каналу).

Канал распространения (информационный канал или канал связи) — среда, используемая для передачи сообщения (информации) от передатчика к приемнику. Иными словами, канал представляет собой пространство между отправителем сообщения и его получателем, характеризуемое определенным расстоянием. При этом информационный канал — среда передачи сообщения в документированном (текстовом) виде, а канал связи служит для обмена информацией, представленной в речевой (звуковой, символьной и т.п.) форме. Во время передачи по каналу связи (информационному каналу) передаваемый сигнал и сообщение, содержащее конфиденциальную информацию, могут быть подвергнуты определенному воздействию. На сигнал воздействуют помехи, он может искажаться при передаче по каналу связи. Воздействие на сообщение может представлять собой попытки овладения содержащейся в нем информацией со стороны злоумышленника (противника, недоброжелателя, конкурента).

Приемник — элемент, выполняющий функцию, обратную функции передатчика. Иными словами, приемник преобразует принятый сигнал и восстанавливает по нему первоначальное сообщение. В рамках системы информационного обмена (в том числе документированной информацией) приемник можно представить в форме объекта, выполняющего также функцию доставки сообщения его получателю.

Получатель информации — объект (лицо), осуществляющий фактический прием, обработку (приведение к документальному виду) и подготовку сообщения для его непосредственного доведения до сведения адресата.

В роли получателя сообщения может выступить работник службы безопасности (режимно-секретного подразделения), функционально отвечающий за получение, учет, регистрацию и доведение до сведения конкретного адресата сообщения, преобразованного в форму документа.

Адресат — должностное лицо (сотрудник предприятия), для которого предназначается передаваемая и принимаемая информация.

При выполнении элементами коммуникационного процесса своих функций возникают объективные возможности негативного воздействия со стороны злоумышленника на передаваемую и принимаемую (обрабатываемую, преобразуемую) информацию. Вследствие этого воздействия появляются каналы утечки конфиденциальной информации независимо от формы ее представления и состояния (существует ли она в форме сообщения или находится в открытом, уже преобразованном для использования виде, обработана или находится в стадии подготовки для доведения до сведения адресата и т.д.).

Основными источниками конфиденциальной информации являются:

- персонал предприятия, допущенный к конфиденциальной информации;

- носители конфиденциальной информации (документы, изделия);

- технические средства, предназначенные для хранения и обработки информации;

- средства коммуникации, используемые в целях передачи информации;

- передаваемые по каналам связи сообщения, содержащие конфиденциальную информацию.

Способы обмена конфиденциальной информацией (например, между сотрудниками предприятия) могут носить как непосредственный (личный) характер, так и характер передачи формируемых на основе информации сообщений посредством технических средств и средств коммуникаций (различных средств и систем связи).

Из существующих способов обмена конфиденциальной информацией необходимо выделить организационные каналы передачи и обмена информацией:

- конфиденциальное делопроизводство (защищенный документооборот);

- совместные работы, выполняемые предприятием по направлениям его производственной и иной деятельности;

- совещания (конференции), в ходе которых обсуждаются вопросы конфиденциального характера;

- рекламная и издательская деятельность;

- различные мероприятия в области сотрудничества с иностранными государствами (их представителями и организациями), связанные с обменом информацией;

- научные исследования, деятельность диссертационных и иных советов учреждений и организаций;

- передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы.

Организационные каналы передачи и обмена конфиденциальной информацией в ходе их функционирования могут быть подвергнуты негативному воздействию со стороны злоумышленников, направленному на получение этой информации.

Данное воздействие, в свою очередь, может привести к возникновению каналов утечки конфиденциальной информации и потребовать от руководства предприятия, руководителей структурных подразделений и персонала принятия мер по защите конфиденциальной информации, направленных на недопущение ее утечки и несанкционированного распространения (утраты носителей конфиденциальной информации).

Для определения необходимых мер по защите информации нужно провести классификацию всех возможных каналов утечки информации в зависимости от направлений и специфики деятельности предприятия, видов конфиденциальной информации, особенностей функционирования системы защиты информации и иных факторов.

Организационные каналы утечки конфиденциальной информации, возникающие в процессе деятельности предприятия, подразделяются следующим образом:

- по источникам угроз защищаемой информации (внешние и внутренние);

- по видам конфиденциальной информации или тайн (государственная, коммерческая, служебная или иная тайна; персональные данные сотрудников предприятия);

- по источникам конфиденциальной информации (персонал, носители информации, технические средства хранения и обработки информации, средства коммуникации, передаваемые или принимаемые сообщения и т.п.);

- по способам или средствам доступа к защищаемой информации (применение технических средств, непосредственная и целенаправленная работа с персоналом предприятия, осуществление непосредственного доступа к информации, получение доступа к защищаемой информации агентурным путем);

- по характеру взаимодействия с партнерами (каналы утечки, возникающие в отсутствие взаимодействия, при осуществлении взаимодействия, в условиях конкурентной борьбы);

- по продолжительности или времени действия (каналы утечки постоянного, кратковременного, а также периодического или эпизодического действия);

- по направлениям деятельности предприятия (каналы утечки, возникающие в обычных условиях или при повседневной деятельности предприятия, при выполнении совместных работ, осуществлении международного сотрудничества, проведении совещаний, выезде персонала за границу, в ходе рекламной и издательской деятельности, при проведении научных исследований или командировании сотрудников предприятия);

- по причинам возникновения каналов утечки информации (действия злоумышленников, ошибки персонала, разглашение конфиденциальной информации, случайные обстоятельства);

- по каналам коммуникации, используемым для передачи, приема или обработки конфиденциальной информации (каналы утечки, возникающие при хранении, приеме-передаче, обработке или преобразовании информации, а также в канале связи, по которому передается информация);

- по месту возникновения каналов утечки информации (каналы утечки, возникающие за пределами территории предприятия или на территории предприятия — в служебных помещениях, на объектах информатизации, объектах связи и в других местах);

- по используемым способам и методам защиты информации (каналы утечки, возникающие при нарушении установленных требований по порядку отнесения информации к категории конфиденциальной, обращения с носителями информации, ограничения круга допускаемых к информации лиц, непосредственного доступа к информации персонала предприятия или командированных лиц, а также по причине нарушения требований пропускного или внутриобъектового режимов).

Задачи по исключению возможных каналов утечки конфиденциальной информации решаются как отдельными должностными лицами (персоналом), так и структурными подразделениями предприятия, создаваемыми и функционирующими по различным направлениям защиты информации. Успешное решение этих задач невозможно без применения совокупности средств и методов защиты информации.

Для более полного представления о системе защиты информации предприятия, силах, средствах, способах, методах защиты информации, мероприятиях, планируемых и проводимых в целях обеспечения информационной безопасности, необходимо рассмотреть основы организационной составляющей системы защиты конфиденциальной информации предприятия как наиболее важного направления деятельности предприятия по защите информации.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Составить краткий перечень организационных каналов утечки конфиденциальной информации.
6. Составить краткий перечень организационных каналов передачи и обмена информацией.
7. Составить перечень возможных угроз для выбранного объекта.
8. Контрольные вопросы.
9. Перечислите основополагающие принципы теории информации.
10. Каковы основы формирования угроз?
11. Перечислите основные источники и способы обмена конфиденциальной информацией. Могут ли они быть каналами утечки информации?
12. Что относится к организационным каналам передачи и обмена информацией?
13. Содержание отчета
14. Краткий перечень организационных каналов утечки конфиденциальной информации.
15. Краткий перечень организационных каналов передачи и обмена информацией.
16. Перечень возможных угроз для выбранного объекта.

Практическая работа № 2.

«Определение состава защищаемой информации»

**Цель:** научиться определять состав защищаемой информации и степень ее секретности и защиты.

1. Общие положения

Определение состава защищаемой информации – это первый шаг на пути построения системы защиты. От того, насколько он будет точно выполнен, зависит результат функционирования разрабатываемой системы. Общий подход состоит в том, что защите подлежит вся конфиденциальная информация, т.е. информация, составляющая государственную тайну (секретная информация), информация, составляющая коммерческую тайну и определяемая собственником (владельцем) часть открытой информации. При этом конфиденциальная информация должна защищаться от утечки и утраты, а открытая – только от утраты.

Защита открытой информации существовала всегда и производилась путем регистрации ее носителей, учета их движения и местонахождения, т.е. создавались безопасные условия хранения. Открытость информации не умаляет ее ценности, а ценная информация нуждается в защите от утраты. Эта защита не должна быть направлена на ограничение общедоступности информации, т.е. не может быть отказа в доступе к информации, но доступ должен осуществляться с соблюдением требований по ее сохранности в соответствии с требованиями обработки и использования (например, библиотека).

Очевидно, что общей основой для отнесения информации к защищаемой является ценность информации, поскольку именно ценность информации диктует необходимость ее защиты. Поэтому критерии отнесения информации к защищаемой являются по существу критериями определения ее ценности.

Применительно к открытой информации такими критериями могут быть:

—необходимость информации для правового обеспечения деятельности предприятия. Это относится к документированной информации, регламентирующей статус предприятия, права, обязанности и ответственность его работников;

—необходимость информации для производственной деятельности (это касается информации, относящейся к научно-исследовательской, проектной, конструкторской, технологической, торговой и другим сферам производственной деятельности);

—необходимость информации для управленческой деятельности, сюда относится информация, требующаяся для принятия управленческих решений, а также для организации производственной деятельности и обеспечения ее

функционирования;

—необходимость информации для финансовой деятельности;

—необходимость информации для обеспечения функционирования социальной сферы;

—необходимость информации как доказательного источника на случай возникновения конфликтных ситуаций;

—важность информации как исторического источника, раскрывающего направления и особенности деятельности предприятия.

Эти критерии обусловливают необходимость защиты открытой информации от утраты. Они же вызывают потребность в защите от утраты и конфиденциальной информации. Однако, основным, определяющим критерием

отнесения информации к конфиденциальной и защиты ее от утечки является возможность получения преимуществ использования информации за счет неизвестности ее третьим лицам.

Преимущества от использования информации, неизвестной третьим лицам, могут состоять в получении выгоды или предотвращении ущерба, иметь, в зависимости от областей и видов деятельности, политические, военные, экономические, моральные и другие характеристики, выражаться количественными и качественными показателями.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Составить перечень информации, подлежащей защите, в выбранной организации.
6. Пояснить, какая информация из перечисленной является открытой, какая закрытой.
7. Контрольные вопросы.
8. Отчего зависит секретность информации?
9. Отчего зависит необходимость защиты информации?
10. Отчего зависит степень защиты информации?
11. Каковы критерии защиты информации?
12. Содержание отчета
13. Выбранная организация.
14. Перечень информации, подлежащей защите.
15. Вывод.

Практическая работа № 3.

«Определение каналов НСД к информации»

**Цель:** научиться определять каналы НСД к информации.

1. Общие положения

Для того чтобы осуществить дестабилизирующее воздействие на конфиденциальную информацию, людям, не имеющим разрешенного доступа к ней, необходимо его получить. Такой доступ называется несанкционированным.

Как правило, несанкционированный доступ бывает преднамеренным и имеет целью оказать сознательное дестабилизирующее воздействие на конфиденциальную информацию.

Несанкционированный доступ (НСД) осуществляется через существующий или специально создаваемый канал доступа, который определяется как путь, используя который, можно получить неразрешенный доступ к конфиденциальной информации.

К каналам несанкционированного доступа к конфиденциальной информации относятся:

1.установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации;

2.вербовка и (или) внедрение агентов;

3.организация физического проникновения к носителям конфиденциальной информации;

4.подключение к средствам отображения, хранения, обработки, воспроизведения и передачи информации, средствам связи;

5.прослушивание речевой конфиденциальной информации;

6.визуальный съем конфиденциальной информации;

7.перехват электромагнитных излучений;

8.исследование выпускаемой продукции, производственных отходов и отходов процессов обработки информации;

9.изучение доступных источников информации;

10.подключение к системам обеспечения производственной деятельности предприятия;

11.замеры и взятие проб окружающей объект среды;

12.анализ архитектурных особенностей некоторых категорий объектов.

Состав реальных для конкретного предприятия каналов несанкционированного доступа к конфиденциальной информации и степень их опасности зависят от вида деятельности предприятия, категорий носителей, способов обработки информации, системы ее защиты, а также от устремлений и возможностей конкурентов. Однако даже если соперники известны, определить их намерения и возможности практически не удается, поэтому защита должна предусматривать перекрытие всех потенциально существующих для конкретного предприятия каналов.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы

Составить перечень НСД к информации в выбранной организации.

1. Контрольные вопросы.
2. Отчего зависят каналы НСД к информации?
3. Какие каналы НСД к информации необходимо перекрывать?
4. Когда необходимо перекрывать каналы НСД к информации?
5. Содержание отчета
6. Выбранная организация.
7. Перечень каналов НСД к информации в выбранной организации.
8. Вывод.

Практическая работа № 4.

«Разработка этапов КСЗИ»

**Цель:** научиться работать по заданному алгоритму, составлять техническое задание.

1. Общие положения

Комплексная система защиты информации (КСЗИ) - совокупность организационных и инженерно-технических мероприятий, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

Объектами защиты КСЗИ является информация, в любом ее виде и форме представления.

В построении КСЗИ можно выделить следующие этапы:

1. Подготовка организационно-распорядительной документации.

2. Обследование информационной инфраструктуры заказчика.

3. Разработка «Плана защиты информации».

4. Разработка «Технического задания на создание КСЗИ».

5. Разработка «Технического проекта на создание КСЗИ».

6. Приведение информационной инфраструктуры заказчика в соответствие с «Техническим проектом на создание КСЗИ».

7. Разработка «Эксплуатационной документации на КСЗИ».

8. Внедрение КСЗИ.

9. Испытание КСЗИ.

10. Проведение государственной экспертизы КСЗИ и получение «Аттестата соответствия».

11. Поддержка и обслуживание КСЗИ.

В построении КСЗИ принимают участие следующие стороны: исполнитель и заказчик, которые связанны непосредственно с каждым этапом разработки. Также требуется участие организатора экспертизы при проведении гос. экспертизы, этапы 4 и 10 включают в себя действие контролирующего органа.

исполнитель и заказчик должны составить договор, в котором подробно описаны порядок, сроки и стоимость работ.

Первым делом проводится исследование и анализ документов, предприятия и помещения заказчика.

1. Подготовка организационно-распорядительной документации

На этом этапе специалисты исполнителя проводят анализ организационно-распорядительных документов заказчика и нормативно-правовых документов в области защиты информации, влияющих на деятельность заказчика.

По результатам выполнения этого этапа исполнитель готовит проекты документов, которые определяют организационную составляющую КСЗИ (проект приказа о создании КСЗИ, проект положения про службу защиты информации, проекты должностных инструкций и процедур и др.), которые утверждаются заказчиком.

2. Обследование информационной инфраструктуры заказчика

На этом этапе специалисты исполнителя проводят обследование (аудит) ИТС заказчика.

Анализируется архитектура системы, её топология и составляющие элементы. Определяются типы пользователей системы, типизируется информация, обрабатываемая в ИТС.

По результатам выполнения этапа исполнитель разрабатывает следующие документы:

- акт обследования ИТС (содержит описание, принципы построения и архитектуру ИТС);

- перечень объектов ИТС подлежащих защите, которые утверждаются заказчиком.

После окончания обследования, опираясь на данные полученные при этом, можно приступить к разработке.

3. Разработка «Плана защиты информации»

По результатам выполнения второго этапа, а именно, основываясь на перечне объектов ИТС, подлежащих защите, исполнитель разрабатывает пакет документов «План защиты информации», которые утверждаются заказчиком:

- документ «Модель угроз информации»;

- документ «Задание на создание КСЗИ»;

- документ «Политика защиты информации»,

4. Разработка «Технического задания на создание КСЗИ»

На этом этапе специалисты исполнителя разрабатывают и согласовывают с заказчиком документ «Техническое задание на создание КСЗИ», который определяет все основные требования к КСЗИ и возможные пути реализации её составляющих элементов.

После согласования «Технического задания на создание КСЗИ» с заказчиком, документ согласовывается с контролирующим органом.

5. Разработка «Технического проекта на создание КСЗИ»

После согласования «Технического задания на создание КСЗИ» с контролирующим органом исполнитель разрабатывает пакет документов «Технический проект на создание КСЗИ».

«Технический проект на создание КСЗИ» представляет собой комплект документов, в который входит часть документов разработанных на предыдущих этапах и ряд новых документов, в которых описано, как именно будет создаваться, эксплуатироваться и, в случае необходимости, модернизироваться КСЗИ.

6. Приведение информационной инфраструктуры заказчика в соответствие с «Техническим проектом на создание КСЗИ».

Особенностью этого этапа является то, что на момент принятия решения о создании КСЗИ стоимость этого этапа является не известной как для заказчика, так и для исполнителя. Также, ввиду большого возможного спектра выполнения работ, на этом этапе существует большая вероятность подключения к его выполнению подрядчиков.

На этом этапе могут выполняться монтажные, строительные, пусконаладочные работы, работы, связанные с установкой необходимых технических или криптографических средств защиты информации, средств физической защиты элементов ИТС (устанавливается необходимое оборудование и программное обеспечение, средства контроля доступа, охранная и пожарная сигнализации) и т.д.

7. Разработка «Эксплуатационной документации на КСЗИ»

На этом этапе исполнитель КСЗИ создаёт пакет документов «Эксплуатационная документация на КСЗИ», который включает:

- инструкции эксплуатации КСЗИ и её элементов;

- процедуры регламентного обслуживания КСЗИ;

- правила и положения по проведению тестирования и анализа работы КСЗИ.

По окончании разработки, при её утверждении мы можем перейти непосредственно к построению системы защиты информации.

8. Внедрение КСЗИ

На этом этапе исполнитель (или подрядчик под авторским надзором исполнителя) проводит все пусконаладочные работы, обучает и инструктирует персонал заказчика правилам и режимам эксплуатации КСЗИ.

После реализации этого этапа внедренная КСЗИ готова к последующему испытанию.

9. Испытание КСЗИ

На этом этапе заказчик при активной поддержке исполнителя проводит предварительные испытания КСЗИ, с целью подтверждения результативности её работы и соответствия положениям, определённым в «Техническом задании на создание КСЗИ».

В процессе испытаний выполняются тестовые задания и контролируются полученные результаты, которые и являются индикатором работоспособности спроектированной КСЗИ.

По результату испытания КСЗИ делается вывод относительно возможности представления КСЗИ на государственную экспертизу.

10. Проведение экспертизы КСЗИ и получение «Аттестата соответствия»

На этом этапе контролирующий орган назначает организатора государственной экспертизы, который проводит независимый анализ (экспертизу) соответствия КСЗИ требованиям, изложенным в документе «Техническое задание на создание КСЗИ», нормативной документации по технической защите информации, а также определяет возможность введения КСЗИ в промышленную эксплуатацию.

Привлечение независимого эксперта (организатора экспертизы) к проведению государственной экспертизы повышает объективность оценки проведенных работ и уменьшает риск нарушений и злоупотреблений в сфере защиты информации.

Любая организация, входящая в Реестр Организаторов экспертиз в сфере ТЗИ, может проводить экспертизы вновь созданных КСЗИ или КСЗИ, «Аттестат соответствия» на которые необходимо продлевать. Реестр организаторов экспертиз ведет контролирующий орган.

Контролирующий орган по результатам проведения государственной экспертизы КСЗИ выдаёт документ «Аттестат соответствия», подтверждающий качество и надёжность построенной КСЗИ.

«Аттестат соответствия» является обязательным для ввода КСЗИ в промышленную эксплуатацию.

После успешного запуска и функционирования КСЗИ остаётся лишь поддерживать её работоспособность и уровень защиты

11. Поддержка и обслуживание КСЗИ

На этом этапе исполнитель может проводить авторский надзор и оказывать консультационную помощь заказчику в эксплуатации КСЗИ, анализе её работы, выработке рекомендаций, и, при необходимости, её модернизации и развитии.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы

Заполните таблицу 1 «Этапы работ по построению подсистем КСЗИ» (приложение 1).

1. Контрольные вопросы.
2. Что такое аудит?
3. Из чего состоит план защиты информации ?
4. Когда необходимо перекрывать каналы НСД к информации?
5. Содержание отчета
6. Этапы разработки КСЗИ.
7. Таблица 1.
8. Вывод.

*Приложение 1*

Таблица 1. Этапы работ по построению подсистем КСЗИ

| № п/п | | Наименование мероприятия | Ответственность | Отчётный документ |
| --- | --- | --- | --- | --- |
| **Подготовительные мероприятия** | | | | |
|  | Обследование, изучение отраслевых стандартов, проектирование, разработка и согласование технического проекта | |  |  |
| **Внедрение** | | | | |
|  | Поставка необходимых технических и программных средств | |  |  |
|  | Установка и настройка программно-технических средств в рамках построения подсистем КСЗИ | |  |  |
|  | Инструктаж технических специалистов Заказчика | |  |  |
|  | Опытная эксплуатация | |  |  |
| **Выпуск исполнительной документации** | | | | |
|  | Разработка результирующей документации на подсистемы КСЗИ | |  |  |

Практическая работа № 5.

«Подбор состава КСЗИ»

**Цель:** научиться определять, на что необходимо обращать внимание, что надо знать для правильной организации системы ИБ.

1. **Общие положения**

На предпроектной стадии выполняется важнейшая работа: изучается объект защиты. Ошибки, допущенные в ходе этой работы, могут существенно снизить эффективность создаваемой СЗ, и, наоборот, тщательно проведенное обследование позволит сократить затраты на внедрение и эксплуатацию системы.

Изучение объекта защиты сводится к сбору и анализу следующей информации:

1)об организации процесса функционирования объекта. В состав этих данных входят сведения, характеризующие:

—график работы объекта и его отдельных подразделений;

—правила и процедуры доступа на объект, в отдельные помещения и к оборудованию персонала и посетителей (регулярный, случайный, ограниченный доступ);

—численность и состав сотрудников и посетителей объекта (постоянный штат, персонал, работающий по контракту, клиенты);

—процедуру доступа на территорию транспортных средств.

Для получения этих данных можно применять следующие способы: анкетирование сотрудников; опрос сотрудников; личное наблюдение; изучение директивных и инструктивных документов. Следует иметь в виду, что ни один из этих способов не дает объективной информации: каждый имеет свои достоинства и недостатки. Поэтому их применяют вместе, в совокупности;

2)об организации транспортных и информационных потоков. В состав этих данных входят сведения, характеризующие:

—пути и организацию транспортировки и хранения материальных ценностей на территории объекта;

—уровни конфиденциальности информации, пути и способы ее обработки и транспортировки (документы, телефонная и радиосвязь и т.п.);

3) об условиях функционирования объекта. В состав этих данных входят сведения, характеризующие:

—пространство, непосредственно прилегающее к территории объекта;

—ограждение периметра территории и проходы;

—инженерные коммуникации, подземные хранилища и сооружения на территории;

—размещение подразделений и сотрудников по отдельным помещениям ( с поэтажными планами);

—инженерные коммуникации в помещениях;

—состояние подвальных и чердачных помещений;

—размещение, конструкции и состояние входов, дверей, окон;

—существующую систему защиты;

—состав и настроение населения, экономические факторы и криминогенную обстановку на прилегающей территории.

На основе результатов анализа всех перечисленных сведений должны быть определены: назначение и основные функции системы защиты; основные виды возможных угроз и субъекты угроз; внешняя среда; условия функционирования системы защиты (наличие энергетических и других ресурсов, естественные преграды и т.п.).

Эти данные рекомендуется систематизировать в виде пояснительной записки, структурных схем и планов.

Целесообразно иметь следующие планы:

1)план территории объекта с указанием расположения всех зданий и других наземных сооружений; подземных сооружений; всех коммуникаций и мест их выхода за территорию объекта; всех ограждений, в том числе по периметру территории объекта, с обозначением их технического состояния на момент обследования; средств защиты (существующей системы, если она имеется);

2)поэтажные планы, где должно быть указано расположение всех помещений с обозначением дверных и оконных проемов, внутренних и наружных (пожарных) лестниц, толщины материала стен и существующих средств защиты; всех коммуникаций с обозначением коммуникационных шкафов и других мест санкционированного доступа к каналам связи и жизнеобеспечения;

3)планы помещений с указанием мест размещения оборудования и других технических средств (телефонов, персональных ЭВМ, принтеров и т.д.); расположения коммуникаций и мест размещения коммутационного оборудования (коробки , розетки и т.п.); функционального назначения и степени конфиденциальности получаемой и обрабатываемой информации; особенностей технологического процесса (для производственных помещений), важных с точки зрения обеспечения безопасности.

На основе этих планов целесообразно подготовить структурные схемы:

—ограждения каждого помещения, указав на ней (схематично) все стены и другие инженерно-технические сооружения, окружающие помещение. Эта схема позволит оценить возможности эшелонирования защиты, выработать рекомендации по рубежам защиты, выбрать и определить зоны безопасности и оценить «прочность» рубежей;

—документооборота (для документов с ограниченным доступом), указав источник и приемник документа; его связи с другими документами; способ подготовки (ручной, машинный); способ транспортировки (с курьером, по телефону, по факсу, по компьютерной сети и т.п.); место хранения; для описания документооборота можно использовать специально разработанные формы.

Каждое предприятие уникально. Поэтому и система защиты конкретного предприятия тоже уникальна. Тем не менее, можно перечислить основные параметры предприятия и показать, каким образом они могут оказывать влияние на разрабатываемую КСЗИ:

—характер деятельности предприятия оказывает влияние на организационно-функциональную структуру КСЗИ, ее состав; состав и структуру кадров СЗИ, численность и квалификацию ее сотрудников; техническое обеспечение КСЗИ средствами защиты; количество и характер мер и мероприятий по ЗИ; цели и задачи КСЗИ;

—состав защищаемой информации, ее объем, способы представления и отображения, технологии обработки: состав и структуру СЗИ; организационные мероприятия по ЗИ; состав технических средств защиты, их объем; состав нормативно-правового обеспечения КСЗИ; методы и способы ЗИ; объем материальных затрат на ЗИ;

—численный состав и структура кадров предприятия: численный состав сотрудников СЗИ; организационную структуру СЗИ; объем затрат на ЗИ; техническую оснащенность КПП; объем организационных мероприятий по ЗИ;

—организационная структура предприятия: организационную структуру КСЗИ; количество и состав сотрудников СЗИ;

—техническая оснащенность предприятия: объем и состав технических средств ЗИ; количество и квалификацию технического персонала СЗИ; методы и способы, размер материальных затрат на ЗИ;

—нормативно-правовое обеспечение деятельности предприятия влияет на формирование нормативно-правовой базы КСЗИ; регулирует деятельность СЗИ; влияет на создание дополнительных нормативно-методических и организационно-правовых документов СЗИ;

—экономическое состояние предприятия (кредиты, инвестиции, ресурсы, возможности) определяет объем материальных затрат на ЗИ; количество и состав сотрудников и квалифицированных специалистов СЗИ; уровень технической оснащенности СЗИ средствами защиты; методы и способы ЗИ;

—режим работы предприятия влияет на режим функциональности КСЗИ, всех ее составляющих; состав технических средств ЗИ; объем затрат на ЗИ; численность персонала СЗИ;

—местоположение и архитектурные особенности предприятия: состав и структуру СЗИ; состав технических средств ЗИ; объем материальных затрат на ЗИ; численный состав и квалификацию сотрудников СЗИ;

—тип производства: организационно-функциональную структуру СЗИ;

—объем производства: размеры материальных затрат на ЗИ; объем технических средств защиты; численность сотрудников СЗИ;

—форма собственности влияет на объем затрат на ЗИ (например, на некоторых государственных предприятиях затраты на защиту информации (СЗИ) могут превышать стоимость самой информации); методы и способы ЗИ.

Организация КСЗИ на каждом конкретном предприятии зависит от параметров рассмотренных характеристик данного предприятия. Эти характеристики определяют цели и задачи КСЗИ, объем ее материального обеспечения, состав и структуру КСЗИ, состав технических средств защиты, численность и квалификацию сотрудников СЗИ т.д. Однако степень воздействия различных характеристик предприятия на организацию КСЗИ различна.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Выполнить анализ характеристик, влияющих на подбор состава КСЗИ.
6. Определить, какие из характеристик имеют большее влияние, а какие меньшее.
7. Контрольные вопросы.
8. Что является основанием для создания КСЗИ?
9. Для чего необходимо изучить планы размещения объектов?
10. Какие характеристики наиболее важны для правильного создания КСЗИ?
11. Как может влиять режим работы предприятия на его ИБ?
12. Как может влиять характер деятельности предприятия на его ИБ?
13. Содержание отчета
14. Перечень данных, необходимых для разработки и создания КСЗИ.
15. Вывод.

Практическая работа № 6.

«Защита корпоративной почты»

**Цель:** научиться обеспечивать комплексный подход к защите корпоративной почтовой системы.

1. Основные положения

Рассмотрим пример построения защищенной корпоративной почтовой системы, включающей в себя как почтовые серверы, так и локальных и удаленных пользователей. Локальные пользователи работают с почтовой системой, находясь внутри корпоративной ИС, а удаленные – вне ИС через сеть Интернет. Взаимодействие между пользователями и серверами осуществляется по протоколам SMTP и POP3.

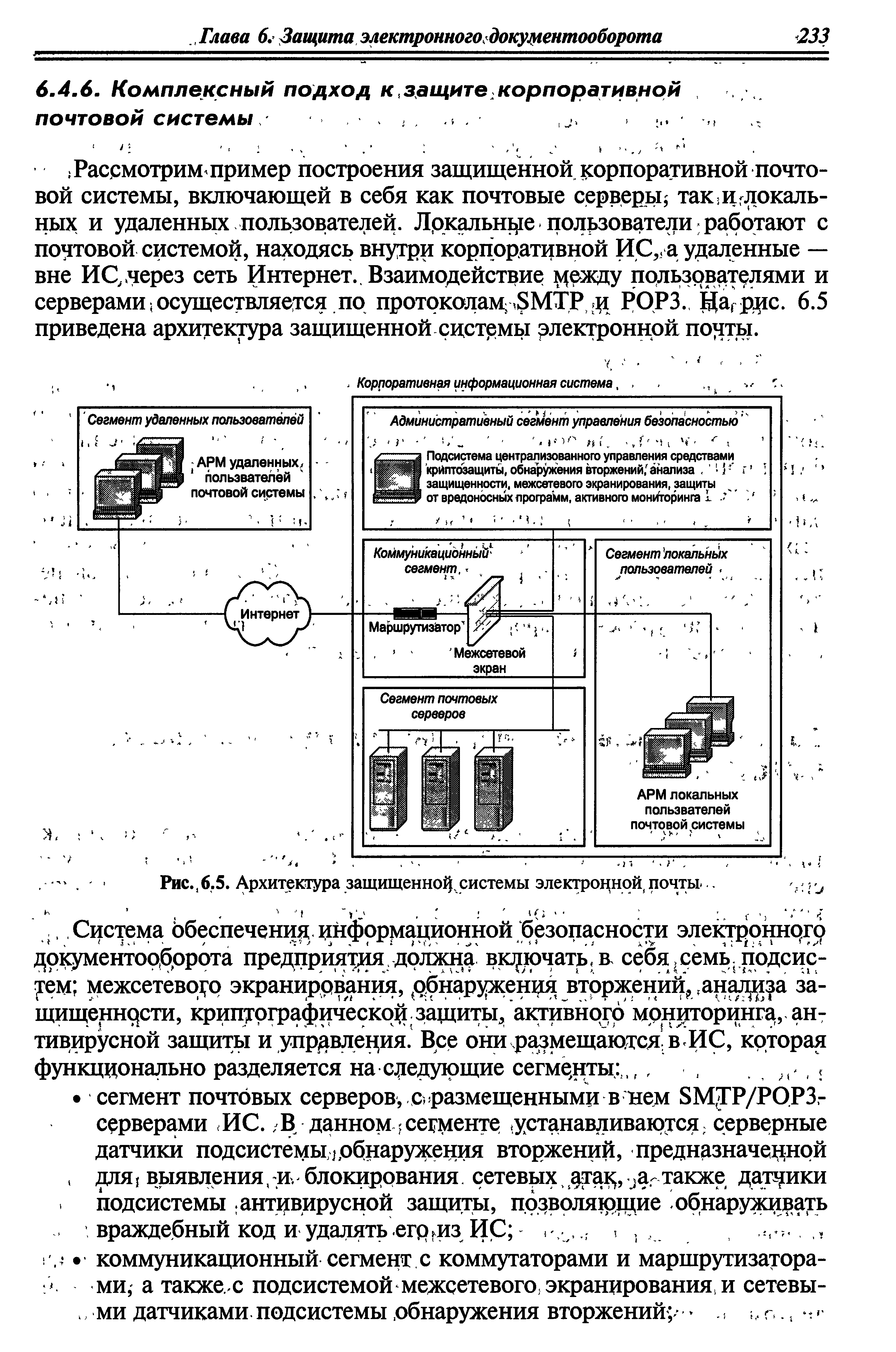


Рисунок 1. Архитектура защищенной системы электронной почты.

Система обеспечения ИБ электронного документооборота предприятия должна включать в себя семь подсистем: межсетевого экранирования (МЭ), обнаружения втрожений, анализа защищенности, криптографической защиты, активного мониторинга, антивирусной защиты и управления. Все они размещаются в ИС, которая функционально разделяется на следующие сегменты:

сегмент почтовых серверов с размещенными в нем SMTP/POP3 – серверами ИС. В данном сегменте устанавливаются серверные датчики подсистемы обнаружения вторжений (СОВ), предназначенной для выявления и блокирования сетевых атак, а также датчики подсистемы антивирусной защиты (АВЗ), позволяющие обнаруживать враждебный код и удалять его из ИС;

коммуникационый сегмент с коммутаторами и маршрутизаторами, а также с подсистемой МЭ и сетевыми датчиками подсистемы обнаружения вторжений;

административный сегмент управления безопасностью ИС с установленными в нем подсистемой анализа защищенности, позволяющей выполнять функции выявления уязвимостей в ПО ИС, подсистемой централизованного управления всем комплексом средств защиты;

сегменты локальных и удаленных пользователей ИС, в которых размещаются антивирусные датчики, специализированнное ПО подсистемы криптографической защиты и датчики системы активного мониторинга. Последние обеспечивают защиту от потенциальной утечки конфиденциальной информации через почтовую систему.

В заключение следует отметить, что, поскольку система электронной почты является одним из важнейших компонентов электронного документооборота любого современного предприятия, нарушение ее функционирования может привести к катастрофическим последствиям для последнего. Именно поэтому ососбое значение приобретает защита данной системы от потенциальных атак, направленных на нарушение конфиденциальности, целостности и доступности передаваемой в ней информации. И лишь комплексный подход позволяет обеспечить высокий уровень ИБ не только почтовой системы, но и всей ИС предприятия в целом.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Выполнить анализ схемы «Архитектура защищенной системы электронной почты».
6. Выполнить анализ функциональных сегментов.
7. Контрольные вопросы
8. По каким протоколам осуществляется взаимодействие между пользователями и серверами?
9. Каковы основные функции протоколов передачи почтовых сообщений?
10. Какой протокол используется сейчас?
11. Возможен ли запрет на передачу почтовых сообщений?
12. Содержание отчета
13. Схема «Архитектура защищенной системы электронной почты».
14. Перечислить функциональные сегменты.
15. Вывод.

Практическая работа № 7.

«Определение обязанностей конечных пользователей и ответственных за ОИБ в подразделениях»

**Цель:** научиться определять и разграничивать обязанности пользователей за ОИБ.

1. **Общие положения**

Достижение некоторого уровня информационной безопасности возможно только при выработке у персонала и пользователей **АС** определенной дисциплины по соблюдению установленных ограничений и правил использования ресурсов и обслуживания компонент АС.

Эта дисциплина немыслима без персональной ответственности всех сотрудников, допущенных к работе с АС, за нарушения установленного порядка (регламента) безопасной обработки информации, правил хранения и использования находящихся в их распоряжении защищаемых ресурсов системы.

Регламентация работы сотрудников предполагает определение для каждой категории пользователей и обслуживающего персонала:

* ***обязательных знаний, действий и процедур,*** необходимых для ОИБ при автоматизированной обработке информации и обслуживании компонент АС;
* ***запрещенных действий,*** которые могут привести к нарушению нормальной работы АС, вызвать непроизводительные затраты ресурсов, нарушить конфиденциальность или целостность хранимой и обрабатываемой информации, нарушить интересы других пользователей;
* ***ответственности*** за нарушение установленных требований и ограничений.

Общие обязанности сотрудников по обеспечению информационной безопасности при работе с ресурсами АС

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированной системы, несет персональную ответственность за свои действия и *обязан:*

* производить обработку защищаемой информации в подсистемах АС в строгом соответствии с утвержденными технологическими инструкциями (техническими порядками) для данных подсистем;
* строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;
* знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;
* хранить в тайне свой пароль (пароли). С установленной периодичностью в соответствии с «Инструкцией по организации парольной защиты автоматизированной системы» менять свой пароль (пароли);
* передавать для хранения установленным порядком свое индивидуальное устройство идентификации ( Touch Memory , Smart Card , Proximity и т.п.).
* другие реквизиты разграничения доступа и носители ключевой  
  информации только руководителю своего подразделения или ответственному за информационную безопасность в подразделении (в пенале, опечатанном своей личной печатью);

• надежно хранить и никому не передавать личную печать и использовать ее только для опечатывания пенала с реквизитами доступа и носителями ключевой информации;

• если сотруднику (исполнителю) предоставлено право защиты (подтверждения подлинности и авторства) документов, передаваемых по технологическим цепочкам в АС, при помощи электронной цифровой подписи (ЭЦП), то он дополнительно обязан соблюдать все требования «Порядка работы с ключевыми носителями»;

• выполнять требования «Инструкции по организации антивирусной защиты в АС» в части касающейся действий пользователей рабочих станций (PC);

• немедленно ставить в известность ответственного за безопасность информации и руководителя подразделения в случае утери носителей ключевой информации, индивидуального устройства идентификации или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

• нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к закрепленной за ним защищенной рабочей станции;

• некорректного функционирования установленных на PC технических средств защиты;

• несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств PC;

• непредусмотренных формуляром PC отводов кабелей и подключённых устройств;

• отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию PC , выхода из строя или неустойчивого функционирования узлов PC или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения:

• присутствовать при работах по изменению аппаратно-программной конфигурации закрепленной за ним рабочей станции, по завершении таких работ проверять ее работоспособность.

Категорически *запрещается:*

*•* использовать компоненты программного и аппаратного обеспечения АС не по назначению (в неслужебных целях);

• самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих станций;

• осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

• записывать и хранить конфиденциальную информацию (сведения ограниченного распространения) на неучтенных носителях (гибких магнитных дисках и т.п.);

• оставлять включенной без присмотра свою рабочую станцию (компьютер), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

• передавать кому-либо свой персональный ключевой кроме ответственного за информационную безопасность или руководителя своего подразделения установленным порядком, делать неучтенные копии ключевого носителя, снимать с него защиту записи и вносить какие-либо изменения в записанные на носитель файлы;

• использовать свои ключи ЭЦП для формирования цифровой подписи любых электронных документов, кроме электронных документов, регламентированных технологическим процессом на его рабочем месте;

• оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, носители ключевой информации, носители и распечатки, содержащие сведения ограниченного распространения;

• умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям информационной безопасности и . возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность ответственного за безопасность информации и руководителя своего подразделения.

*Обязанности ответственного за обеспечение безопасности информации в подразделении*

Ответственный за обеспечение информационной безопасности (администратор информационной безопасности - АИБ) подразделения (технологического участка) назначается из числа штатных сотрудников подразделения по представлению его руководителя, согласованному с подразделением обеспечения информационной безопасности.

АИБ непосредственно подчиняется руководителю подразделения, в штате которого он состоит, и осуществляет контроль за выполнением требований организационно-распорядительных документов по обеспечению безопасности информации при ее обработке на компьютерах подразделения дополнительно к своим непосредственным обязанностям.

Методическое руководство работой администратора информационной безопасности осуществляется подразделением обеспечения информационной безопасности.

*Администратор информационной безопасности обязан:*

• знать перечень установленных в его подразделении компьютеров и перечень задач, решаемых с их использованием;

• обеспечивать постоянный контроль за выполнением сотрудниками подразделения установленного комплекса мероприятий по обеспечению безопасной автоматизированной обработки, информации;

• контролировать целостность печатей (пломб) на устройствах защищенных компьютеров подразделения;

• немедленно сообщать руководителю подразделения и сотрудникам подразделения обеспечения безопасности информации об обнаруженных фактах (попытках) несанкционированного доступа к информации и техническим средствам, и принимать необходимые меры по пресечению нарушений;

• обеспечивать соблюдение сотрудниками своего подразделения, подразделений автоматизации и ОИБ утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств PC и серверов («Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС»), при их техническом обслуживании и отправке в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях) и лично присутствовать при выполнении данных работ (участвовать в работах);

• вести «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств PC подразделения»;

• хранить формуляры защищенных PC , контролировать их соответствие реальным конфигурациям PC и вести учет изменений их аппаратно-программной конфигурации (заявки, на основании которых были • произведены данные изменения);

• вести «Журнал учета ключевых носителей подразделения», хранить, осуществлять прием и выдачу ключевых носителей ответственным исполнителям подразделения в строгом соответствии с установленным порядком работы с ключевыми носителями, осуществлять контроль за правильностью использования ключевых носителей сотрудниками своего подразделения (технологического участка);

• осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов (в соответствии с Планом ОНРВ);

• проводить работу по выявлению возможных каналов неправомерного вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам ПЭВМ. При выявлении таковых сообщать о них руководству подразделения и специалистам подразделения ОИБ;

• инструктировать сотрудников подразделения по вопросам ОИБ и правилам работы с используемыми средствами зашиты информации.

*Администратор информационной безопасности имеет право:*

• требовать от сотрудников подразделения - пользователей АС соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности информации в АС;

• инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АС;

• обращаться к руководителю подразделения с требованием прекращения работы на рабочих станциях при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;

• подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты на своем участке работы;

• обращаться в подразделение обеспечения информационной безопасности за необходимой технической и методологической помощью в своей работе.

*Права исполнителя*

Исполнитель должен иметь право обращаться к ответственному за информационную безопасность своего подразделения за консультациями по вопросам использования ключевого носителя и по вопросам обеспечения информационной безопасности технологического процесса.

Исполнитель имеет право требовать от ответственного за информационную безопасность своего подразделения и от своего непосредственного руководителя создания необходимых условий для выполнения перечисленных выше требований.

Исполнитель имеет право представлять свои предложения по совершенствованию мер защиты на своем участке работы.

*Ответственность за нарушения*

Для создания необходимой юридической основы процедур привлечения сотрудников к ответственности за нарушения в области ОИБ необходимо, чтобы:

• в Уставе организации, во всех положениях о структурных подразделениях и в функциональных (технологических) обязанностях всех сотрудников, участвующих в процессах автоматизированной обработки информации, были отражены требования по обеспечению информационной безопасности при работе в АС;

• каждый сотрудник (при приеме на работу) подписывал Соглашение-обязательство о соблюдении установленных требований по сохранению государственной, служебной и коммерческой тайны, а также об ответственности за нарушение правил работы с защищаемой информацией в АС;

• все пользователи, руководящий и обслуживающий персонал АС были ознакомлены с перечнем сведений, подлежащих защите, в части их касающейся (в соответствии со своим уровнем полномочий);

• доведение требований организационно-распорядительных документов по вопросам ОИБ до лиц, допущенных к обработке защищаемой информации, осуществлялось руководителями подразделений под роспись.

Сотрудники организации несут ответственность по действующему законодательству за разглашение сведений, составляющих (государственную, банковскую, коммерческую) тайну, и сведений ограниченного распространения, ставших им известными по роду работы.

Любое грубое нарушение порядка и правил работы в АС сотрудниками структурных подразделений должно расследоваться. К виновным должны применяться адекватные меры воздействия.

Нарушения установленных правил и требований по ОИБ являются основанием для применения к сотруднику (исполнителю) административных мер наказания, вплоть до увольнения и привлечения к уголовной ответственности.

Мера ответственности сотрудников за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, должна определяться с учетом нанесенного ущерба, наличия злого умысла и других факторов по усмотрению руководства.

*Для реализации принципа персональной ответственности сотрудников за свои действия необходимы:*

• индивидуальная идентификация сотрудников и инициированных ими процессов при работе в АС, т.е. установление за ними уникальных идентификаторов пользователей, на основе которых будет осуществлять разграничение доступа и регистрация событий;

• проверка подлинности соответствия пользователей и сотрудников (аутентификация) на основе паролей, ключей, специальных устройств, биометрических характеристик личности сотрудников и т.п.;

• регистрация (протоколирование) работы механизмов контроля доступа пользователей к ресурсам информационных систем с указанием даты и времени, идентификаторов пользователя и запрашиваемых им ресурсов, вида взаимодействия и его результата;

• оперативная реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Выполнить анализ обязанностей сотрудников
6. Проанализировать действия, за которые сотрудник несет ответственность.
7. Привести примеры нарушений информационной безопасности пользователем и администратором.
8. Контрольные вопросы.
9. Что является основанием обвинять сотрудника в нарушении информационной безопасности?
10. Для чего работодателю необходимо иметь юридические документы в области ИБ?
11. В чем заключаются возможные ошибки работодателя при приеме на работу?
12. В чем заключаются ошибки сотрудника при работе с информацией?
13. Что такое ключевой носитель? Для чего он служит?
14. Что необходимо сделать пользователю и администратору при подозрении на нарушение информационной безопасности?
15. Что необходимо для реализации принципа персональной ответственностисотрудников за свои действия?
16. Содержание отчета
17. Перечень обязанностей и прав сотрудников.
18. Ответственность за нарушение ИБ.
19. Примеры нарушения информационной безопасности пользователем и администратором
20. Вывод.

Практическая работа № 8.

«Определение ошибок кадрового обеспечения КСЗИ»

**Цель:** научиться определять причины нарушений ОИБ сотрудниками и определить способы предотвращения допуска таких сотрудников к информационной системе.

1. Общие положения

Подбор персонала

Большинство систем не может функционировать без участия человека, что является верным и для комплексных систем ЗИ. Группа обеспечения таких систем, с одной стороны, ее необходимый элемент, с другой — он же может быть причиной и движущей силой нарушения и преступления. Сотрудник предприятия является определяющей фигурой в обеспечении сохранности сведений. Он может выступать в качестве создателя интеллектуальной собственности предприятия (совершенствуя технологию, создавая какие-либо товары и др.). При этом значительная часть ценнейшей для предприятия информации не отражается в технической документации, а остается в голове. И в дальнейшем, накопив опыт, многие из них потенциально готовы в будущем реализовать свой идей на практике. Кроме того, если сотрудник привлекается к закрытым работам, руководитель предприятия вынужден предоставить ему наиболее ценную информацию, полученную другим работником.

Проведя анализ статистических данных по отечественным и зарубежным источникам, можно сделать вывод, что около 70 % (а по некоторым источникам эта цифра еще выше) всех нарушений, связанных с безопасностью информации, совершаются именно сотрудниками предприятия. Можно выделить 5 причин этого факта:

1) при нарушениях, вызванных безответственностью, сотрудник целенаправленно или случайно производит какие-либо действия по компрометации информации, связанные со злым умыслом;

2) бывает, что сотрудник предприятия ради самоутверждения (для себя или коллег) затевает своего рода игру «пользователь — против системы». И хотя намерения могут быть безвредными, будет нарушена сама практика безопасности. Такой вид нарушений называется зондированием системы;

3) нарушение может быть вызвано и корыстным интересом. В этом случае сотрудник будет пытаться целенаправленно преодолеть систему защиты для доступа к хранимой, перерабатываемой и обрабатываемой на предприятии информации;

4) за рубежом известна практика переманивания специалистов, так как это позволяет ослабить конкурента и дополнительно получить информацию о предприятии. Таким образом, не обеспечив закрепление лиц, осведомленных в секретах, талантливых специалистов, невозможно в полной мере сохранить секреты предприятия. Вопросам предупреждения текучести кадров в зарубежных фирмах уделяют большое внимание. Представители японской администрации рассматривают компанию как совокупность различных ресурсов. При этом люди стоят на первом месте, т. к. именно они воплощают технологию и в них в первую очередь заключается конкурентоспособная сила фирмы. То есть текучесть кадров четвертая причина;

5) специалист, работающий с конфиденциальной информацией, испытывает отрицательное психическое воздействие, обусловленное спецификой этой деятельности. Поскольку сохранение чего-либо в тайне противоречит потребности человека в общении путем обмена информацией, сотрудник постоянно боится возможной угрозы утраты документов, содержащих секреты. Выполняя требования режима секретности, сотрудник вынужден действовать в рамках ограничения своей свободы, что может привести его к стрессам, психологическим срывам, а как результат — нарушении безопасности информации.

Понимая ведущую роль кадров в сохранении секретов, руководителям предприятия важно помнить, какие личные качества человека не способствуют сохранению доверенной ему тайны. То есть причины нарушения безопасности информации связаны с психологическими особенностями человека, его личными качествами, следовательно, и способы предотвращения перечисленных нарушений вытекают из анализа побудительных мотивов: тщательный подбор персонала, подготовка персонала, поддержание здорового рабочего климата, мотивация и стимулирование деятельности сотрудников.

В любой профессиональной деятельности есть стабильные составляющие и переменные, связанные с конкретными условиями, в которых эта деятельность осуществляется. При подборе кадров важно принимать во внимание обе составляющие, т. е. дается описание психологических характеристик, соблюдение которых необходимо для выполнения определенных профессиональных обязанностей. В психограмму включаются требования, предъявляемые профессиональной деятельности, к психологическим процессам (памяти, воображению, восприятию), психическим состояниям (усталости, апатии, стрессу), вниманию как состоянию сознания, эмоциональным (сдержанность, индифферентность) и волевым (настойчивость, импульсивность) характеристикам. Некоторые из этих психологических требований являются основными, главными, без них вообще невозможна качественная деятельность.

Психологическое несоответствие требованиям профессии особенно сильно проявляется в сложных ситуациях, когда требуется мобилизация всех личностных ресурсов для решения сложных задач. Поэтому это особенно важно в рамках комплексной системы защиты информации.

Но описание психологических требований недостаточно, чтобы, ориентируясь только на них, подбирать человека для работы. При подборе кадров необходимо ориентироваться не только на отдельные характеристики психики, а на черты личности как ее системные свойства. Выделим наиболее результативные методы изучения личности:

— изучение жизненного пути личности;

— изучение мнения коллектива, в котором работает личность;

— изучение ближайшего окружения личности;

— создание ситуации, наиболее подходящей для проявления профессионально важных качеств и свойств;

— изучение высказывания личности о собственной роли в делах коллектива.

К качествам, соответствующим работе в таких условиях, относятся: честность, добросовестность, принципиальность (строгое следование основным правилам), исполнительность, пунктуальность, дисциплинированность, эмоциональная устойчивость (самообладание), стремление к успеху и порядку в работе, самоконтроль в поступках и действиях, правильная самооценка собственных способностей и возможностей, осторожность, умение хранить секреты, тренированное внимание и неплохая память.

Качества, не способствующие сохранению доверенной тайны: эмоциональное расстройство, неуравновешенность поведения, разочарование в себе, отчужденность от коллег по работе, недовольство своим служебным положением, ущемленное самолюбие, эгоистичные интересы, нечестность, употребление наркотиков и алкоголя, постепенно разрушающих личность.

Подготовка персонала для работы в новых условиях

С целью максимальной эффективности использования вновь принятого на работу человека, необходимо, принимая на работу нового сотрудника, не ограничиваться ознакомлением его с техникой безопасности, режимами работы, с рабочим местом, навыками владения средствами и предметами труда. В качестве примера влияния адаптационного периода рассмотрим результаты исследования феномена «летунов», т. е. людей, часто меняющих профессию или место работы, которые показывают, что в начале их трудового пути, как правило, был неудачный опыт адаптации к предприятию и коллективу. В результате, столкнувшись с первыми трудностями на работе, с первыми сложностями, с конфликтами, такой человек в силу особенностей психики уходит от этих трудностей путем увольнения с работы по собственному желанию.

Причина этих явлений условия, не способствующие адаптации вновь принятого работника. Такими неблагоприятными условиями могут быть условия обыденные, удобные, даже рациональные с точки зрения работников, хорошо приспособившихся к окружающей их производственной среде. Поэтому трудности новичков не замечаются. Условно сложная адаптация может быть разделена на виды: профессиональная, социально-организационная, социально-психологическая.

Профессиональная адаптация — это адаптация к самой трудовой деятельности со всеми обеспечивающими ее предметными и временными составляющими. Она характерна при обстоятельствах, возникающих при первом знакомстве человека с условиями его новой работы. Эта адаптация неизбежна при всех изменениях, происходящих на предприятии или на рабочем месте.

Социально-организационная адаптация включает в себя знакомство с работой органов управления и обеспечения работы предприятия (отдел кадров, администрация и т. д.), со сферой жизни коллектива, связанной с бытом и отдыхом.

Социально-психологическая адаптация связана с вхождением нового работника в первичный коллектив.

Мотивация — это процесс побуждения себя и других к деятельности для достижения личных целей или целей организации. Мотивация, определяющая отношение к деятельности, — это личное побуждение к деятельности, т. е. побуждение, основанное на потребностях личности, ее ценностных ориентациях, интересах. Среди мотивов в первую очередь следует выделить интерес к деятельности, чувство долга, стремление к профессиональному росту. Мотивация на основе интереса связана с удовлетворением стремления к знанию и развитию. Причем существует два аспекта этой мотивации: интерес к деятельности и интерес к самому себе как субъекту, овладевшему этой деятельностью. Продуктивность мотивации, основанной на интересе к деятельности, связана с содержательностью, т. е. той стороной деятельности, которая вызывает наибольший интерес. Мотивация на основе чувства долга связана с потребностью соответствовать требованиям организации, ее нуждам. Особое значение составляют мотивы, основывающиеся на принципе взаимной ответственности и требовательности, характерные для коллективных отношений. Мотивация на основе стремления к профессиональному росту может проявиться когда человек уже достаточно прочно чувствует себя как субъект деятельности. Тогда обостряется желание быстрее достичь некоторых стандартов деятельности или превзойти их.

Напрашивается способ мотивации, связанный со стимулированием или другими словами, мотивация через потребности. Поскольку характер каждого человека — это соединение самых разнообразных черт, то, следовательно, существует огромное число человеческих потребностей, которые, по мнению каждого человека, приводят к удовлетворению его потребностей. Например, потребность в утверждении собственного «я» одного человека можно удовлетворить, признав его лучшим работником отдела, а удовлетворить аналогичную потребность кого-то другого — означает признать лучшим фасоном его одежды, объявив всем, что он одевается лучше других в группе.

По теории Маслоу, все потребности человека можно расположить в виде строго иерархичной структуры. Верхний уровень образует вторичные потребности. К ним относятся потребности в самовыражения, уважения и социальные. А первичные потребности — безопасности, защищенности и физиологические потребности, образуют нижние уровни. Этим он хотел сказать, что потребности нижних уровней требуют удовлетворения и влияют на поведение человека прежде, чем на мотивации начнут сказываться потребности более высоких уровней. В каждый конкретный момент времени человек будет стремиться к той потребности, которая для него является наиболее важной или сильной. Прежде чем потребность следующего Уровня станет решающим фактором в поведении человека, должна быть удовлетворена потребность более низкого уровня. Для того чтобы следующий, более высокий уровень потребностей начал влиять на поведение человека, не обязательно удовлетворять полностью потребности более низкого уровня, т. е., хотя в данный момент одна из потребностей может преобладать, деятельность человека стимулируется не только ею. И хотя для большинства людей их основные потребности располагались приблизительно в том же порядке, как мы рассмотрели, однако бывают исключения.

Перечислим методы удовлетворения потребностей высших уровней.

I. Социальные потребности:

1) давайте сотрудникам такую работу, которая позволяет им общаться;

2) создавайте на рабочих местах дух единой компании;

3) проводите с подчиненными периодические совещания;

4) не старайтесь разрушить возникшие неформальные группы;

5) создавайте условия для социальной активности членов организации вне ее рамок.

II. Потребности в уважении:

1) предлагайте подчиненным более содержательную работу;

2) обеспечьте им положительную обратную связь с достигнутым результатом;

3) высоко оценивайте и поощряйте достигнутые подчиненными результаты;

4) привлекайте подчиненных к формулированию целей и выработке решений;

5) делегируйте подчиненным дополнительные права и обязанности;

6) продвигайте подчиненных по карьерной лестнице;

7) обеспечьте обучение и переподготовку, которая, повышает уровень компетентности.

III. Потребности в самовыражении:

1) обеспечивайте подчиненных возможностью для обучения и развития, которые позволили бы полностью использовать их потенциал;

2) давайте подчиненным сложную и важную работу, требующую их полной отдачи;

3) поощряйте и развивайте у подчиненных творческие способности.

Большое значение для мотивации имеет климат в коллективе. И если все-таки дело дошло до увольнения, очень важно, чтобы работник ушел, не затаив зла. Возможно, необходимо поговорить с ним, выяснить причины ухода и в том случае, если уход связан с конфликтом, чувством неудовлетворенности и т. д., потребовать еще раз разобраться в ситуации, и тем самым, возможно, поправить положение.

1. Оснащение занятия
2. Методические рекомендации.
3. Порядок выполнения работы
4. Проанализировать действия сотрудников отдела кадров.
5. Проанализировать возможные действия сотрудников, принятых на работу, направленные на нарушение ИБ организации.
6. Контрольные вопросы.
7. Что является основанием обвинять сотрудника в нарушении информационной безопасности?
8. Для чего работодателю необходимо тщательно выбирать сотрудников?
9. В чем заключаются возможные ошибки отдела кадров при приеме на работу?
10. В чем заключаются ошибки работодателя при работе с сотрудником?
11. Что такое мотивация? Для чего она служит? К чему может привести отсутствие правильной мотивации на работе?
12. Кем чаще всего совершаются нарушения ИБ?
13. Для чего сотрудники нарушают ИБ? Почему они ее нарушают?
14. Содержание отчета
15. Перечень методов изучения личности.
16. Виды адаптации.
17. Мотивация.
18. Вывод.

**Практическая работа № 9.**

«Разработка кодекса корпоративного поведения»

**Цель:** получение практических навыков разработки кодекса корпоративного поведения.

1. Основные положения

Корпоративное поведение – понятие, охватывающее разнообразные действия, связанные с хозяйственным управлением и управлением обществами.

Кодекс корпоративного поведения предназначен

Большинство компаний используют для создания и поддержания организационной культуры правила внутреннего трудового распорядка. Стоит заметить, что они не отвечают современным требованиям и к тому же не являются мотивационным инструментом.

Кодекс корпоративного поведения может выполнять три основные функции:

1) репутационная;

2)управленческая;

3)функция развития корпоративной культуры.

Как правило, кодексы содержат две части:

—идеологическую (миссия, цели, ценности);

—нормативную(стандарты рабочего поведения).

При этом идеологическая часть может не включаться в содержание кодекса.

Большинство компаний используют для создания и поддержания организационной культуры правила внутреннего трудового распорядка. Стоит заметить, что они не отвечают современным требованиям и к тому же не являются мотивационным инструментом. По соотношению доступности и результативности формирования и поддержания позитивной организационной культуры внедрение кодекса корпоративного поведения является наиболее эффективным. В таком кодексе должны быть максимально четко обозначены приоритетные цели и задачи организации, ее миссия, а также расставлены акценты во внутренних и внешних отношениях, с сотрудниками, клиентами, руководством. Это элемент традиционной корпоративной культуры, улучшающий и укрепляющий психологическую атмосферу коллектива.

Кодекс корпоративного поведения может выполнять три основные функции:

1) репутационная;

2) управленческая;

3) функция развития корпоративной культуры.

Репутационная функция кодекса заключается в формировании доверия к организации со стороны референтных внешних групп (государства, заказчиков, клиентов, конкурентов и т. д.). Наличие у компании кодекса корпоративного поведения становится общемировым деловым стандартом.

Управленческая функция кодекса состоит в регламентации поведения в сложных этических ситуациях. Повышение эффективности деятельности сотрудников осуществляется путем:

— регламентации приоритетов во взаимодействии со значимыми внешними группами;

— определения порядка принятия решений в сложных этических ситуациях;

— указания на неприемлемые формы поведения.

Корпоративная этика, кроме того, является составной частью организационной культуры и кодекс корпоративного поведения — значимый фактор ее развития. Кодекс призван выявлять приоритетные для организации ценности и доводить их до каждого сотрудника, как новичка, так и опытного профессионала. В идеале персонал будет ориентироваться на единые цели и тем самым повышать корпоративную идентичность, приверженность общему делу.

Содержание кодекса компании определяется, прежде всего, ее особенностями, структурой, задачами развития, установками ее руководителей.

Как правило, кодексы содержат две части:

— идеологическую (миссия, цели, ценности);

— нормативную (стандарты рабочего поведения).

При этом идеологическая часть может не включаться в содержание кодекса.

В профессионально однородных организациях (банки, исследовательские центры, консультационные компании) часто используются кодексы, описывающие в первую очередь узкоспециальные дилеммы. Эти кодексы являются производными от кодексов профессиональных сообществ. Соответственно, содержание таких кодексов в первую очередь регламентирует поведение сотрудников в сложных профессиональных этических ситуациях. В банковской деятельности, например, это доступ к конфиденциальной информации о клиенте и сведениям об устойчивости банка. Кодекс описывает правила обращения с такой информацией, запрещает использовать сведения в целях личного обогащения.

В первую очередь здесь решаются управленческие задачи. Дополнение такого кодекса главами о миссии и ценностях компании способствует развитию корпоративной культуры. При этом кодекс может иметь значительный объем и сложное специфическое содержание и адресоваться всем сотрудникам компании.

В больших неоднородных корпорациях сочетание всех трех функций становится сложным. С одной стороны, существует ряд политик и ситуаций, традиционно закрепляемых этическими кодексами в международной практике. Это политики по отношению к клиентам, поставщикам, подрядчикам. Описание ситуаций, связанных с возможными злоупотреблениями, например взятки, подкуп, хищения, обман, дискриминация. Исходя из управленческой функции, кодекс описывает стандарты образцового поведения в таких ситуациях. Такой кодекс имеет значительный объем и достаточно сложное содержание. Адресация его всем группам сотрудников в условиях значительной разницы в образовательном уровне и социальном статусе сотрудников затруднена. В то же время развитие корпоративной культуры компании требует единого кодекса для всех сотрудников — он должен задавать единое понимание миссии и ценностей компании для каждого сотрудника.

По сути, декларативный вариант — это только идеологическая часть кодекса без регламентации поведения сотрудников. При этом в конкретных ситуациях сотрудники сами должны ориентироваться, как им себя вести, исходя из базовых этических норм, обозначенных в кодексе. Однако в ряде случаев сотрудникам трудно оценить этическую правомерность конкретного поступка исходя из общих принципов.

Таким образом, декларативный вариант кодекса решает в первую очередь задачи развития корпоративной культуры. При этом для предоставления кодекса международному сообществу и решения конкретных управленческих задач необходима разработка дополнительных документов.

В развернутых вариантах кодекса с подробной регламентацией этики поведения сотрудников фиксируется конкретные поступки персонала в отдельных областях, где риск нарушений наиболее высок или возникают сложные этические ситуации. Эти регламенты описываются в виде политик в отношении заказчиков, государства, клиентов, политической деятельности, конфликта интересов, безопасности труда.

При этом большой объем и сложность содержания таких кодексов определяют их выборочную адресацию (см. табл. 3). В большинстве компаний такие кодексы разрабатываются для высшего и среднего менеджмента и не являются всеобщим документом, объединяющим всех сотрудников.

Итак, каждая компания определяет собственные задачи, Для решения которых она намерена использовать такой инструмент, как кодекс корпоративного поведения. Но создание кодекса, естественно, не ограничивается только написанием текста документа. Существует специфика исполнения подобных документов: заставить исполнять этический кодекс нельзя. Поэтому для того, чтобы он действительно работал, еще на этапе его создания необходимо предусмотреть процедуры, включающие в процесс разработки документа по возможности всех сотрудников компании. Только при условии принятия каждым сотрудником кодекса корпоративного поведения он будет реально исполняться.

Основным решением проекта стала идея «улицы с двусторонним движением»:

1) «сверху вниз» — определение базовых ценностей и целей высших руководителей, разработка на их основе проекта;

2) «снизу вверх» — каждому сотруднику предоставлялась возможность стать соавтором Кодекса через его обсуждение и внесение собственных предложений.

Общий план разработки состоит из трех этапов.

1-й этап. Проектирование. Разработка проекта кодекса с основным акцентом на цели и ценности, среди которых важное место отведено контролю безопасности и сохранности конфиденциальной информации. Здесь же указано отношение первых лиц и высшего руководства к существующей в организации проблематике этического характера.

Для этого проводится анализ существующих кодексов других компаний в контексте их применения.

Определялись базовые ценности и цели данной организации, а также наиболее актуальные сферы применения кодекса.

В итоге должна быть сформирована концепция кодекса, в том числе его идеология, формат, сферы применения и создается предварительный проект текста.

2-й этап. Обсуждение. Обсуждение проекта кодекса в трудовых коллективах, во всех подразделениях организации и сбор предложений по доработке текста кодекса и системы его исполнения.

На этом этапе важно провести работу по следующим позициям:

— разъяснение сотрудникам смысла, значения и сфер применения кодекса;

— привлечение рядовых сотрудников к процессу создания Кодекса;

— создание позитивного общественного мнения в отношении кодекса среди персонала, а также подготовка менеджмента и квалифицированных сотрудников как ресурса по внедрению кодекса в практику ежедневной деятельности.

Процесс обсуждения включает в себя такие элементы, как:

— очная и заочная формы обсуждения проекта кодекса, которые позволяет сотрудникам стать соавторами кодекса;

— оригинальная методика групповой работы по обсуждению проекта кодекса, как с руководителями, так и с неформальными лидерами общественного мнения, которые бы инициировали дальнейшее обсуждение документа в трудовых коллективах;

— оперативная обработка и передача данных очного обсуждения для незамедлительного использования в параллельно идущем заочном обсуждении в корпоративных средствах массовой информации;

— интерактивная модульная схема информационной кампании, позволяющая вести в диалоговом режиме разъяснение ключевых смыслов кодекса и отвечать на самые актуальные вопросы.

Очное обсуждение ориентировано на включение в диалог работников, заинтересованных в будущем своей организации, у которых есть что высказать и предложить ради повышения общего морального климата.

Заочное обсуждение (информационная кампания в корпоративных и федеральных СМИ, а также в корпоративных виртуальных сетях) теоретически может охватить более высокий процент сотрудников, чем физически осуществимо при очном учете масштабов корпорации. В период обсуждения Кодекса должны быть задействованы все доступные средства, печатные издания, освещение темы на корпоративном сайте организации, в стенгазетах.

Обратная связь

Само обсуждение кодекса уже является началом его внедрения. Процесс обсуждения служит основой для поиска общих интересов сотрудников и руководства, построения единой ценностно-целевой картины и развития диалога между сотрудниками и руководством.

3-й этап. Интеграция. Этот этап включает анализ всех поступивших предложений, внесение изменений в содержание проекта, выработка механизмов исполнения и внедрения документа.

После обсуждения документа проводится анализ предложений, полученных от сотрудников, и на его основе корректируется содержание кодекса.

Кроме того, на этом этапе применяется схема построения механизмов внедрения и исполнения кодекса, основанная на изучении опыта других компаний, а также на предложениях сотрудников.

Итогом третьего этапа проекта становится создание окончательного варианта текста кодекса, его полиграфическое исполнение и распространение среди персонала.

Спустя некоторое время возможна ситуация, когда однажды принятый кодекс корпоративного поведения потеряет актуальность, морально устареет. В этом случае высшему руководству требуется созвать комиссию по его пересмотру, и в случае решения о неизбежности внесения изменений, разработать новый проект кодекса, с обязательным учетом прошлого опыта.

Формирование позитивной корпоративной культуры с учетом специфики безопасности затрагивает изменение таких существенных представлений, как внутренний психологический климат коллектива, фундаментальные ценности, устоявшиеся паттерны поведения, совокупность формальных и неформальных требований к персоналу в виде норм, и, наконец, общие представления представителей коллектива об окружающей среде, организации и индивидуальности каждого из сотрудников.

Все эти понятия являются составляющими организационной культуры и обусловливают деятельность, осуществляемую сознательно или неподконтрольно отдельными нормами субкультур организации, которые должны быть скорректированы таким образом, чтобы не противостоять первичным ценностям безопасности, установленным основной доминирующей культурой, не находиться в оппозиции к ним.

Чтобы действия, преследующие цели укрепления механизмов безопасности, были адекватно восприняты и приняты коллективом, они должны быть не только разумны, но и соответствовать базовым представлениям сотрудников о правильности, чему способствует изучение и понимание корпоративной культуры. Подсознательного неприятия или даже открытого противодействия политике безопасности можно избежать, если своевременно провести тщательное наблюдение, в ходе которого должен быть выявлен преобладающий тип корпоративной культуры каждого структурного подразделения, который может варьироваться в зависимости от функциональных, возрастных, профессиональных, географических или иных особенностей. Также крайне важно определить неформальных лидеров выявить наиболее авторитетные субкультуры, значительно влияющие на внутреннюю жизнедеятельность организации. Важно выбрать наиболее эффективно работающую субкультуру и использовать ее в качестве исходной позиции для введения инноваций.

1. Оснащение занятия
2. Методические рекомендации.
3. Порядок выполнения работы
4. Составить кодекс корпоративного поведения по отношению к ОИБ.
5. Ответить на контрольные вопросы.
6. Оформить отчет.
7. Контрольные вопросы
8. Что такое кодекс корпоративного поведения?
9. Для чего необходим данный документ?
10. Как кодекс корпоративного поведения влияет на ИБ?
11. Содержание отчета
12. Функции кодекса корпоративного поведения.
13. Содержание кодекса.
14. Кодекс корпоративного поведения по отношению к ОИБ
15. Вывод.

Практическая работа № 10.

«Выявление проблем ЗИ на предприятии и определение механизмов КСЗИ»

**Цель:** получение навыков выявления проблем ЗИ на предприятии и выбора систем обнаружения вторжений.

1. Общие положения:

Система обнаружения вторжений (СОВ) (Intrusion Detection System) предназначены для регистрации враждебного трафика, обнаружения атак, сигнализации системного администратора о уже начавшейся атаке и ее отражении. Подобные средства появились не так давно и поэтому в России пока не производятся. В таблице 1 представлены некоторые из существующих на мировом рынке СОВ.

Системы обнаружения вторжений делятся на три типа:

* + уровень хоста;
  + уровень сети;
  + процедурные.

Системы первого типа занимаются ведением журнала регистрации, наблюдением за процессами, а также контролем за целостностью двоичного кода.

Системы уровня сети занимаются тем, что анализируют проходящий трафик, сравнивают его с известными сигнатурами атак и принимают решение о вторжении в случае совпадения кода. В этом случае делается запись журнале и извещается системный администратор. Ну и конечно же СОВ пытается сама противодействовать атаке.

Процедурная же модель систем обнаружения вторжений занимается тем же, что и система сетевого уровня, а также фиксирует и исследует проходящую работу, пытаются адаптироваться к данной сети.

Система обнаружения вторжений является неплохим дополнением к МЭ и в ряде случаев занимаются облегчением труда системных администраторов, но в тоже время обладает существенным недостатком, коим обладают и антивирусные сканеры: СОВ не способны обнаружить неизвестные вторжения, пока не будут обновлены сигнатуры.

Таблица 1. Краткая характеристика продуктов СОВ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Компания-производитель** | **Продукт** | **Тип продукта** | **Платформа** |
| 1 | Axent Technologies | NetProwler | Уровня сети | Windows NT |
| 2 | Cisco System | Cisco Secure IDS 4210/4230  Cisco Secure IDS Module | Уровня сети  То же | Устройство  Cayalyst 6000 |
| 3 | Computer Associates International | ETrust Intrusion Detection | То же | Windows NT |
| 4 | CyberSafe | Centrax Host Engine  Centrax Network Engine | Уровень хоста  Уровня сети | AIX, Solaris, Windows NT/2000  AIX, Solaris, Windows NT/2000 |
| 5 | Hiverworld | Armor | Уровня сети | Устройство |
| 6 | Intrusion.com | SecureNet Pro  Kane Security Enterprise | То же  Уровень хоста | Linux  Solaris, Cisco IOS, Cisco Secure IDS, Check Point Firewall-1, RealSecure, Windows NT |
| 7 | Internet Security System | RealSecure Server Sensor | Гибридный | Windows NT |
| 8 | Network Associates | CyberCop Monitor | Гибридный | Windows NT |
| 9 | Network Flight Recorder | NTF | То же | Устройство |
| 10 | Свободно распространяемые | Snort  Pakemon  Shadow | То же  То же  То же | Unix, Windows NT  Unix  Unix |

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Выбрать СОВ из приведенных в таблице 1.
6. Найти описание СОВ в интернете.
7. Дать краткую характеристику.
8. Оформить отчет.
9. Контрольные вопросы
10. Что означает «уровень хоста», «уровень сети»?
11. Для каких устройств предназначены СОВ?
12. Для каких платформ существуют СОВ?
13. Какие преимущества и недостатки СОВ?
14. Содержание отчета:
15. Описание СОВ в общем виде.
16. Описание выбранного СОВ.

**Практическая работа № 11**

**« Определение возможных чрезвычайных ситуаций на предприятии»**

**Цель:** получение практических навыков определения чрезвычайных ситуаций на предприятии и их влияния на информационную безопасность.

1. Общие положения

Все ситуации, возникающие в процессе функционирования, можно условно разделить на две группы: нормальные и ненормальные. Ненормальные ситуации, в свою очередь, делятся на аварийные, потенциально аварийные и нештатные. Любая из этих ситуаций требует принятия ответных мер, направленных на:

* сокращение комплекса факторов, влияющих на возникновение чрезвычайной ситуации;
* защиту людских, информационных, материальных и других ресурсов от негативного воздействия, нанесения ущерба и уничтожения;
* обеспечение работы объекта во время и после реализации нештатной ситуации.

Чрезвычайную ситуацию (ЧС) можно определить как комплекс событий, проявление и протекание которых могут привести к нарушению нормального функционирования КСЗИ либо создать условия для проявления различных форм уязвимости защищаемой информации.

Чрезвычайные ситуации можно классифицировать по различным признакам.

1. По масштабам сферы действия:

* межгосударственные;
* общегосударственные;
* местные;
* объектовые.

1. По виду наносимого ущерба:

* ЧС с прямым ущербом;
* ЧС с косвенным ущербом;
* ЧС, представляющие угрозу жизни людей;
* ЧС, приводящие к нарушению экологического равновесия, уничтожению материальных ресурсов и т.д.

1. По времени и динамике развития:

* стратегические ЧС, приводящие к катастрофическим последствиям;
* медленнотекущие ЧС;
* ЧС оперативного плана, с выраженной динамикой развития.

4. По вероятности возникновения:

* прогнозируемые;
* трудно прогнозируемые;
* непрогнозируемые.

1. По степени сложности при ликвидации последствий:

* легкоустранимые ЧС;
* ЧС, требующие определенных временных и ресурсных затрат для их ликвидации;
* трудно устранимые ЧС;
* ЧС, требующие особых средств и мероприятий для ликвидации их последствий

1. Оснащение занятия

Методические рекомендации.

1. Порядок выполнения работы
2. Составить перечень возможных ЧС на выбранном объекте (не менее трех).
3. Описать возможные последствия данных ЧС, влияющие на ИБ.
4. Описать влияние данных ЧС на ИБ.
5. Контрольные вопросы
6. Возможно ли предотвратить ЧС на предприятии?
7. Возможно ли предотвратить последствия ЧС на предприятии?
8. Какие ЧС наиболее опасные для ИБ?
9. Какими могут быть последствия ЧС для ИБ на предприятии?
10. На каком этапе проектирования КСЗИ нужно предусматривать возможность ЧС на предприятии?
11. Отчего зависит вероятность возникновения ЧС?
12. Содержание отчета
13. Перечень возможных ЧС на выбранном объекте (не менее трех).
14. Возможные последствия данных ЧС, влияющие на ИБ.
15. Влияние данных ЧС на ИБ.

**Практическая работа № 12**

**«Составление перечня информации для проведения аудита информационной безопасности»**

**Цель:** получение практических навыков определения информации на предприятии, необходимой для проведения аудита информационной безопасности.

1. Общие положения

Риск ИБ – потенциальная возможность использования определенной угрозой уязвимостей актива или группы активов для причинения вреда организации.

Уязвимость - слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ - совокупность условий и факторов, которые могут стать причиной нарушений целостности, доступности, конфиденциальности информации.

Информационный актив – это материальный или нематериальный объект, который:

- является информацией или содержит информацию,

- служит для обработки, хранения или передачи информации,

- имеет ценность для организации.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Прочитать в электронной системе поиска «Кодекс: Техэксперт» ГОСТ Р ИСО 19011-2012. «Руководящие указания по аудиту систем менеджмента» приложение В.
6. Составить перечень информации, необходимой для проведения аудита на предприятии по вашему варианту.
7. Контрольные вопросы
8. Для чего необходим аудит ИБ на предприятии?
9. Возможно ли снизить риск ИБ после проведения аудита?
10. Какие документы и информация наиболее важные для проведения аудита ИБ?
11. Содержание отчета
12. Перечень информации, необходимой для проведения аудита ИБ.
13. Ответы на контрольные вопросы

**Практическая работа № 13**

**«Разработка инструкции при работе с ПК для сотрудников организации»**

**Цель:** получение практических навыков составления инструкции при работе сотрудников организации с персональным компьютером (ПК) для обеспечения информационной безопасности.

1. Общие положения

Основываясь на положениях ФЗ-149 «Об информации, информационных технологиях и о защите информации» (с изменениями на 2 декабря 2019 года) (редакция, действующая с 13 декабря 2019 года) необходимо составить инструкцию по соблюдению мер информационной безопасности при работе с персональным компьютером для сотрудников организации. В инструкции обязательно отразить элементы работы с ключевыми носителями информации, работе с паролями, документами, действиях во время перерывов при работе с ПК и другие.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Прочитать в электронной системе поиска «Кодекс: Техэксперт» ФЗ-149 «Об информации, информационных технологиях и о защите информации» (с изменениями на 2 декабря 2019 года) (редакция, действующая с 13 декабря 2019 года).
6. Составить инструкцию для соблюдения мер по информационной безопасности для сотрудников организации по вашему варианту.
7. Контрольные вопросы
8. Для чего необходима инструкция по ИБ для пользователей ПК на предприятии?
9. Возможно ли снизить риск ИБ с помощью данной инструкции?
10. Какие еще меры необходимо применять сотрудникам организации для обеспечения ИБ организации?
11. Содержание отчета
12. Инструкция для сотрудников.
13. Ответы на контрольные вопросы

**Практическая работа № 14**

**«Разработка инструкции по составлению пароля»**

**Цель:** получение практических навыков составления пароля.

1. Общие положения

Основываясь на положениях Р 50.1.111-2016 «Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации» необходимо составить инструкцию по составлению пароля для сотрудников организации.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Прочитать в электронной системе поиска «Кодекс: Техэксперт» Р 50.1.111-2016 «Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации».
6. Составить инструкцию по составлению пароля для сотрудников организации.
7. Контрольные вопросы
8. Для чего необходима инструкция по составлению пароля?
9. Возможно ли снизить риск ИБ с помощью данной инструкции?
10. Какие еще меры необходимо применять сотрудникам организации для обеспечения ИБ организации?
11. Содержание отчета
12. Инструкция для сотрудников.
13. Ответы на контрольные вопросы

**Практическая работа № 15**

**«Составление перечня нормативно-методического обеспечения ИБ организации»**

**Цель:** получение практических навыков составления перечня нормативно-методического обеспечения ИБ организации.

1. Общие положения

Нормативно-методическое обеспечение КСЗИ представляет собой комплекс положений законодательных актов, нормативов, методик, правил, регламентирующих создание и функционирование КСЗИ, взаимодействие подразделений и лиц, входящих в структуру системы, а также статус органов, обеспечивающих функционирование КСЗИ.

К содержанию нормативно-методических документов по ЗИ предъявляются требования. ИС должна быть защищена путем внедрения продуманных правил безопасности. СЗИ должна использовать набор правил для того, чтобы определить, может ли данный субъект получить доступ к данному объекту. Для предприятия целесообразно внедрение правил обеспечения безопасности и получение полномочий, с помощью которых можно было бы эффективно реализовать доступ к конфиденциальной информации. Пользователи, не обладающие соответствующими полномочиями, не должны получать доступ к конфиденциальной информации. Кроме того, необходимо применение дискриминационных методов управления, обеспечивающих доступ к данным только для некоторых пользователей или пользовательских групп, например, исходя из служебных обязанностей. Информационная система должна быть защищена с помощью правил безопасности, которые ограничивают доступ к объектам (файлы, приложения) со стороны субъектов (пользователи). Нормативные документы, определяющие порядок защиты, должны удовлетворять следующим требованиям:

— соответствовать структуре, целям и задачам предприятия;

— описывать общую программу обеспечения безопасности, включая вопросы эксплуатации и усовершенствования;

— перечислять возможные угрозы информации и каналы ее утечки, результаты оценки опасностей и рекомендуемые защитные меры;

— определять ответственных за внедрение и эксплуатацию всех средств защиты;

— определять права и обязанности пользователей, причем таким способом, чтобы этот документ можно было использовать в суде при нарушении правил безопасности.

Прежде чем приступить к разработке документов, определяющих порядок ЗИ, нужно провести оценку угроз, определить информационные ресурсы, которые целесообразно защищать в первую очередь, и подумать, что необходимо для обеспечения их безопасности. Правила должны основываться на здравом смысле. Целесообразно обратить внимание на следующие вопросы:

— принадлежность информации; об информации обязан заботиться тот, кому она принадлежит;

— определение важности информации; пока не определена значимость информации, не следует ожидать проявлений должного отношения к ней;

— значение секретности; как пользователи хотели бы защищать секретность информации? Нужна ли она им вообще?

Если право на сохранение тайны будет признано в вашей организации, то может ли она выработать такие правила, которые обеспечивали бы права пользователей на защиту информации?

Состав нормативно-методического обеспечения может быть определен следующим образом: законодательная база, руководящие методические документы и информационно-справочная база. К первому компоненту относятся: законы, указы президента, постановления правительства, кодексы (гражданский, уголовный, административный), госты. Во второй компонент могут входить документы министерств и ведомств, а также документы, разработанные на предприятиях по вопросам защиты информации. В состав информационно-справочной базы входят словари, каталоги, специализированные журналы, справочники, электронные базы данных. Нормативно-методическая документация должна содержать следующие вопросы защиты информации:

— какие информационные ресурсы защищаются;

— какие программы можно использовать на служебных компьютерах;

— что происходит при обнаружении нелегальных программ или данных;

— дисциплинарные взыскания и общие указания о проведении служебных расследований;

— на кого распространяются правила;

— кто разрабатывает общие указания;

— точное описание полномочий и привилегий должностных лиц;

— кто может предоставлять полномочия и привилегии;

— порядок предоставления и лишения привилегий в области безопасности;

— полнота и порядок отчетности о нарушениях безопасности и преступной деятельности;

— особые обязанности руководства и служащих по обеспечению безопасности;

— объяснение важности правил (пользователи, осознающие необходимость соблюдения правил, точнее их выполняют);

— дата ввода в действие и даты пересмотра;

— кто и каким образом ввел в действие эти правила.

План защиты информации может содержать следующие сведения:

— назначение ИС;

— перечень решаемых ИС задач;

— конфигурация;

— характеристики и размещение технических средств и программного обеспечения;

— перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в ИС;

— требования по обеспечению доступности, конфиденциальности, целостности различных категорий информации;

— список пользователей и их полномочий по доступу к ресурсам системы;

— цель защиты системы и пути обеспечения безопасности ИС и циркулирующей в ней информации;

— перечень угроз безопасности ИС, от которых требуется защита, и наиболее вероятных путей нанесения ущерба;

— основные требования к организации процесса функционирования ИС и мерам обеспечения безопасности обрабатываемой информации;

— требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;

— основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности ИС (особые обязанности должностных лиц ИС);

— цель обеспечения непрерывности процесса функционирования ИС, своевременность восстановления ее работоспособности и чем она достигается;

— перечень и классификация возможных кризисных ситуаций;

— требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов. и т. п.);

— обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы;

— разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;

— определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;

— определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т. п.);

— определение порядка разрешения споров в случае возникновения конфликтов.

1. Оснащение занятия
2. Методические рекомендации.
3. Персональный компьютер.
4. Порядок выполнения работы
5. Составить перечень документов.
6. Контрольные вопросы
7. Для чего необходим перечень нормативно-методического обеспечения ИБ на предприятии?
8. Какие документы наиболее важны для обеспечения ИБ?
9. Содержание отчета
10. Перечень нормативно-методического обеспечения ИБ на предприятии.
11. Ответы на контрольные вопросы

**Информационное обеспечение обучения**

Основные источники:

1. Мельников В.П. Информационная безопасность: учебник / В.П. Мельников, А.И. Куприянов; под ред. В.П. Мельникова. - 2-е изд., перераб. и дпо. - Москва: КНОРУС, 2018. - 268 с. - (Среднее профессиональное образование)
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – Москва : Питер, 2020. – 992 с. : ил. – (Учебник для вузов. Стандарт третьего поколения).

Дополнительные источники:

1. Олифер, В.Г. Основы сетей передачи данных [Электронный ресурс] : учебное пособие / В.Г. Олифер, Н.А. Олифер. — Электрон. дан. — Москва : , 2016. — 219 с. — Режим доступа: https://e.lanbook.com/book/100346.