|  |
| --- |
| Государственное бюджетное профессиональное образовательное учреждение «Пермский техникум промышленных и информационных технологий имени Б.Г.Изгагина» |

**ОТЧЕТ**

|  |  |  |
| --- | --- | --- |
| по специальности |  | МДК.02.02 Организация и технология защиты информации |

|  |  |
| --- | --- |
| Выполнил: | Какоткин В.С. |
|  |  |
| Преподаватель: | Болотова О.Г. |

г. Пермь**Цель работы:**

1. Изучить РЕГЛАМЕНТ ПРОВЕРКИ НОСИТЕЛЕЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ДЕЛОПРОИЗВОДСТВЕ и ответить на поставленные вопросы;
2. Составить акт проверки наличия носителей конфиденциальной информации;
3. Составить схему источников дестабилизирующего воздействия на информацию;
4. Определить источники и носители информации по методике выявления способов воздействия на информацию.

**Анализ Регламента проверки носителей   
конфиденциальной информации в делопроизводстве**

Виды проверок:

* регламентированными (периодическими);
* нерегламентированными (непериодическими).

Технология проведения проверок носителей конфиденциальной информации

* подготовку квартальной или годовой проверки;
* проверку в службе конфиденциальной документации;
* проверку на рабочих местах исполнителей;
* оформление и анализ результатов проверки.

Принципы проведения проверок носителей конфиденциальной информации

* Охват проверочными операциями всех подлежащих проверке носителей, всех учетных форм, в которых зафиксированы проверяемые реквизиты, и всех необходимых сопроводительных (оправдательных) материалов о движении носителей.
* Проведение проверок наличия носителей по схеме "сначала документ, потом учетные данные на него" (от документа к формам учета), что обеспечивает большую возможность обнаружения неучтенных конфиденциальных носителей.
* Фиксация конечных результатов проверок.

**Технология проведения проверок носителей конфиденциальной информации**

Технологическая схема проверки наличия носителей информации включает в себя следующие процедуры:

1. подготовку квартальной или годовой проверки;
2. проверку в службе конфиденциальной документации;
3. проверку на рабочих местах исполнителей;
4. оформление и анализ результатов проверки.

В процессе проведения квартальной проверки наличия носителей конфиденциальной информации контролируется сохранность традиционных и электронных документов, находящихся на исполнении у сотрудников организации и неподшитых в дела. Одновременно проверяется соблюдение сотрудниками установленного порядка работы с конфиденциальными материалами, их хранения, правильности ведения внутренней описи документов, находящихся у исполнителя, своевременности и полноты ежедневной сдачи всех носителей в службу конфиденциального делопроизводства (КД). Проверка ведется только в присутствии самого сотрудника.

В процессе проведения годовой проверки наличия конфиденциальных носителей контролируется сохранность всех традиционных и электронных документов, как находящихся на исполнении, так и исполненных, подшитых в дела независимо от времени их поступления, получения или издания. Отсутствие конфиденциального носителя информации у сотрудника, которому он был выдан, считается утратой этого носителя. В подобном случае комиссия составляет соответствующий акт и немедленно докладывает об утрате первому руководителю организации для принятия решения. Акт составляется также в случае обнаружения в базе данных компьютера сотрудника или несанкционированной сохраненной копии электронного документа.

**Принципы проведения проверок носителей конфиденциальной информации**

При проведении проверок необходимо руководствоваться следующими принципами.

1. Охват проверочными операциями всех подлежащих проверке носителей, всех учетных форм, в которых зафиксированы проверяемые реквизиты, и всех необходимых сопроводительных (оправдательных) материалов о движении носителей.

2. Проведение проверок наличия носителей по схеме "сначала документ, потом учетные данные на него (от документа к формам учета), что обеспечивает большую возможность обнаружения неучтенных конфиденциальных носителей.

3. Фиксация конечных результатов проверок.

**Cхема источников дестабилизирующего воздействия на информацию**



Рисунок 1 – Источники дестабилизирующего воздействия

**Источники и носители информации по методике выявления способов воздействия на информацию.**

К ним относятся:

1. Люди;
2. Технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи;
3. Системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации;
4. Технологические процессы отдельных категорий промышленных объектов;
5. Природные явления.

Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются люди, которые делятся на следующие категории:

* сотрудники данного предприятия;
* лица, не работающие на предприятии, но имеющие доступ к защищаемой информации предприятия в силу служебного положения (из вышестоящих, смежных (в том числе посреднических) предприятий, контролирующих органов государственной и муниципальной власти и др.);
* сотрудники государственных органов разведки других стран и разведывательных служб конкурирующих отечественных и зарубежных предприятий;
* лица из криминальных структур, хакеры.

В части соотношения с видами и способами дестабилизирующего воздействия на информацию эти категории людей подразделяются на две группы: имеющие доступ к носителям данной защищаемой информации, техническим средствам ее отображения, хранения, обработки, воспроизведения, передачи и системам обеспечения их функционирования и не имеющие такового.

Отличия в конкретно применяемых видах и методах Дестабилизирующего воздействия на информацию между названными группами людей (при однотипности видов и методов) обусловлены преследуемыми целями. Основной целью второй группы людей является несанкционированное получение (хищение) информации, являющейся конфиденциальной. Уничтожение, искажение, блокирование информации стоят на втором плане, а нередко и не являются целью. Дестабилизирующее воздействие со стороны этой группы людей в подавляющем большинстве случаев является преднамеренным (умышленным, сознательным). К тому же, для того чтобы осуществить дестабилизирующее воздействие на конфиденциальную информацию, людям, входящим в эту группу, нужно иметь канал несанкционированного доступа к ней.

Для первой группы людей несанкционированное получение конфиденциальной информации вообще не является целью в силу наличия у них доступа к такой информации. Целями дестабилизирующего воздействия со стороны этой группы являются разглашение, несанкционированное, уничтожение, блокирование, искажение информации (перечислены в последовательности, соответствующей степени интенсивности воздействия, от большей к меньшей). Хищение информации также присуще для данной группы, но оно является не целью, а средством для осуществления уничтожения или разглашения информации. Предметом воздействия со стороны этой группы является не только конфиденциальная информация (хотя она в первую очередь), но и защищаемая часть открытой информации. Воздействие со стороны людей, включенных в данную группу, может быть как преднамеренным, так и непреднамеренным (ошибочным, случайным). Следует, однако, оговорить, что по объектам доступа эта группа неоднородна по своему составу. В нее входят люди, имеющие доступ и к носителям защищаемой информации, и к средствам отображения, хранения, обработки, воспроизведения и передачи информации (ко всем или части из них), и к системам обеспечения функционирования этих средств; люди, имеющие доступ только к информации и (иногда или) к средствам ее обработки (всем либо отдельным); люди, допущенные только к системам обеспечения функционирования средств.

Самым многообразным этот источник является потому, что ему, по сравнению с другими источниками, присуще значительно большее количество видов и способов дестабилизирующего воздействия на информацию.

Самым опасным этот источник является потому, что, во-первых, он самый массовый, во-вторых, воздействие со стороны носит не эпизодический, постоянный характер, в-третьих, как уже отмечалось, его воздействие может быть не только непреднамеренным, как со стороны других источников, но и преднамеренным.

Технические средства отображения, хранения, обработки, воспроизведения, передачи информации и средства связи являются вторым по значению источником дестабилизирующего воздействия на защищаемую информацию в силу их многообразия, а также существующих с их стороны способов дестабилизирующего воздействия. К этому источнику относятся:

* электронно-вычислительная техника;
* электрические и автоматические пишущие машинки, и копировально-множительная техника;
* средства видео- и звукозаписывающей и воспроизводящей техники;
* средства телефонной, телеграфной, факсимильной, громкоговорящей передачи информации;

Третий источник дестабилизирующего воздействия на информацию включает системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования.

К четвертому источнику относятся технологические процессы объектов ядерной энергетики, химической промышленности, радиоэлектроники, а также объектов по изготовлению некоторых видов вооружения и военной техники, которые изменяют естественную структуру окружающей объект среды.

Пятый источник — природные явления — включает составляющие: стихийные бедствия и атмосферные явления.