МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационных технологий и управления

Кафедра информационных технологий автоматизированных систем

**ОТЧЕТ**

По лабораторной работе №7

«Защита данных военных сил и МВД»

|  |  |  |
| --- | --- | --- |
| Выполнил |  | Проверил: |
| ст. гр. 328501 |  | Ярмолик В. И. |
| Суворов В. В. |  |  |

Минск 2023

**1 ЦЕЛЬ РАБОТЫ**

Изучить способы защиты информации и данных в МВД и военных силах.

**2 ДАННЫЕ МВД**

Министерство внутренних дел держит личные данные миллионов людей Беларуси, которые используются и в других органах. Органы МВД разграничивают полномочия, обеспечивают информационную безопасность, чтобы каждый пользователь информационной системы получил именно те данные, которые ему положены в рамках решения функциональных обязанностей. Поэтому в ведомстве переосмыслен подход и выработана многоуровневая модель обеспечения информационной безопасности.

Различают 5 уровней:  
1 Организационный: разработка локальных нормативно-правовых актов, методических рекомендаций, консультации с пользователями информационных систем, чтобы дать им доступ и рассказать об основных аспектах работы.

2 Прикладной: установка программного обеспечения на тех ресурсах информационных систем, которые работают с персональными данными. Дальше идут сами ресурсы и базы данных с персональной информацией. Это резервное копирование, восстановление в случаях сбоя, обеспечение работоспособности ресурсов. Все информационные системы в основном работают в режиме 24/7 по мере необходимости.

3 Системный уровень: обновление операционных систем, чтобы убрать уязвимость и корректно их настроить.

4 Сетевой уровень: предусматривает организацию каналов передачи данных, закрытие этих каналов, чтобы не было каких-то вмешательств в линии передачи данных.

5 Физический: обеспечение бесперебойного функционирования всего оборудования.

Если обеспечивается должный порядок на каждом уровне, тогда обеспечивается информационная безопасность как самих систем, так и персональных данных.

**3 ДАННЫЕ ВОЕННЫХ СИЛ**

Меры, которые могут быть применены в целях защиты информации и обеспечения безопасности, делятся на две группы:

1. Защита информационных систем от повреждения и информации от

утечки и перехвата;

1. Защита психики личного состава от намеренного информационно-психологического воздействия.

Эти меры должны приниматься в совокупности, опираясь на все новейшие научные разработки и программные продукты.

Первая группа мер:

1. Защита объектов дислокации войск и расположенных в них АСУ и элементов компьютерной техники от огневого поражения или иного намеренного выведения из строя;
2. Защита систем от удаленного проникновения в них противника, в частности с установлением программных продуктов, обеспечивающих полную защиту периметра от проникновений, например, *DLP*-систем и *SIEM*-систем;
3. Защита информации, носящей характер государственной или военной тайны, от утечек или намеренного похищения;
4. Радиоэлектронная защита;
5. Использование защищенных моделей компьютеров и программных средств, которые не могут быть повреждены заранее созданными проблемами в их кодах;
6. Развитие средств электронной разведки;
7. Использование социальных сетей для намеренного дезинформационного воздействия на противника;
8. Защита систем связи.

Ко второй группе мер относится:

1. Предохранение психики войск от намеренного психологического воздействия;
2. Корректировка информации, транслируемой потенциальным противником.

Для разработки и реализации комплекса этих мер необходимо создание отдельных подразделений, действующих в сфере информационной безопасности.

Так основные способы защиты включают в себя:

1. Криптография: Использование сильных алгоритмов шифрования для защиты конфиденциальной информации в пути и в хранилище. Криптография включает в себя как симметричные (одинаковый ключ для шифрования и дешифрования), так и асимметричные (различные ключи для шифрования и дешифрования) методы.
2. Сегментация сетей: Разделение сетевых ресурсов на сегменты с разными уровнями доверия, что помогает ограничивать распространение угроз и повышать безопасность.
3. Безопасные коммуникации: Защита военных коммуникаций от перехвата и атак с помощью шифрования и других технологий.
4. Аутентификация и авторизация: Применение строгих систем контроля доступа, включая биометрическую аутентификацию и двухфакторную аутентификацию.
5. Физическая безопасность: Обеспечение безопасности физического доступа к важным объектам, серверным центрам и другим инфраструктурным элементам.
6. Контроль съемных носителей данных: Ограничение использования и подключения съемных устройств, таких как *USB*-флешки, для предотвращения утечек данных.
7. Аудит и мониторинг: Проведение систематического мониторинга сетевой активности и аудита для выявления подозрительных действий и инцидентов безопасности.
8. Функциональная безопасность: Гарантирование безопасности работы важных систем и технологий для предотвращения их компрометации.
9. Обучение и обучение персонала: Регулярные тренинги и обучение сотрудников по вопросам безопасности для снижения риска социальной инженерии и неправильного обращения с данными.
10. Строгая политика управления доступом: Установление четких правил и ограничений для управления доступом к чувствительной информации.

**4 ВЫВОД**

Защита и безопасность данных необходима во всех сферах обработки данных, особенно в таких масштабных, стратегически важных органах как МВД и военные силы. Для этого используется и разрабатывается множество методов, как эту информацию можно засекретить, зашифровать, предотвратить внешнее вмешательство и т.д.