**Основные требования к информационной безопасности**

Общепринятым методом войти в систему во время атаки на информационные ресурсы является вход при помощи официального логин-запроса. Технические средства, позволяющие выполнить вход в нужную систему, – логин и пароль.

При авторизации стоит придерживаться нескольких общих требований:

1. Обеспечение высокого уровня безопасности. Терминал (точка входа активного пользователя в информационную систему), не имеющий специальной защиты, используется исключительно на том предприятии, где доступ к нему получают работники с наивысшим квалификационным уровнем. Терминал, который установлен в публичном общественном месте, должен всегда иметь уникальный логин и пароль сложного уровня. Это необходимо для того, чтобы обеспечить полноценную информационную безопасность.
2. Наличие систем контроля за общим доступом в помещение, где установлено оборудование, на котором хранится информация предприятия, в архивные помещения и другие места, которые являются уязвимыми с точки зрения информационной безопасности.

Если используются удаленные терминалы, в компании должны соблюдаться такие основные требования:

* Все удаленные терминалы обязаны посылать запрос на ввод логина и пароля. Доступ без ввода пароля должен быть запрещен.
* Если есть возможность, то в качестве обеспечения информационной защиты надо применить схему так называемого возвратного звонка от модема. Только она, используя уровень надежности автоматической телефонной станции, дает подтверждение, что удаленные пользователи получили доступ с конкретного номера телефона.

К главным требованиям по информационной безопасности во время идентификации пользователей по логину и паролю относятся следующие:  
у каждого пользователя должен быть пароль высокого уровня сложности для того, чтобы войти в систему;

* пароли надо подбирать очень тщательно, информационная емкость пароля должна соответствовать общим стандартам (наличие заглавных букв, цифр);
* пароль, установленный по умолчанию, надо изменить до того, как будет произведен официальный запуск системы;
* каждая ошибка входа в систему обязательно записывается в общий журнал архивных событий, анализируется спустя конкретный промежуток времени; это необходимо для того, что администратор мог выявить причину возникновения ошибок;
* на момент отправления пакетов с подтверждением или отказом введения пароля система должна быть приостановлена на пять секунд, благодаря этому хакеры не смогут вводить большое количество разных паролей, чтобы обойти информационную защиту.

Для полноценного обеспечения защиты от взлома пароля надо выполнить ряд требований:

* для обеспечения защиты информации потребуется подключить двухэтапную аутентификацию;
* подключить защиту от изменения паролей – хакеры могут попытаться воспользоваться таким способом войти в информационную систему, как «забыли пароль – изменить».

Чтобы специалисты могли обеспечить информационную безопасность всех данных, руководитель компании обязан проводить инструктажи для работников на тему «Предотвращение утечки информации». Важно, чтобы работники предприятия знали о возможных опасностях, которые могут возникнуть в случае, если персональные компьютеры на какой-либо промежуток времени остаются без присмотра. Особенно это касается тех ПК, которые не имеют закрытых от постороннего доступа паролей и находятся в публичном месте или офисе.

|  |  |  |
| --- | --- | --- |
| [Назад](1.html) | [Главная](file:///C:\practice2\index.html) | [Вперёд](3.html) |