УТВЕРЖДАЮ
И.о.начальника
Тамбовоблохотуправления

_____В.Н.Разводов
«1» апреля 2013 г.

Политика парольной защиты Управления по охране, контролю и регулированию использования объектов животного мира Тамбовской области

Настоящая политика регламентирует организационно-техническое обеспечение процессов формирования, использования, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИС Управления, а также процесса контроля действий пользователей и обслуживающего персонала системы при работе с паролями.

Общие положения

Управление по охране, контролю и регулированию использования объектов животного мира Тамбовской области (далее - Управление) производит обработку персональных данных в соответствии с положением об обработке персональных данных в администрации области, утвержденным постановлением администрации области от 26.06.2012 № 760 "Об организации работ по защите персональных данных в администрации области" и правилами обработки персональных данных в администрации области, утвержденными постановлением администрации области от 24.12.2012 № 1644 "Об утверждении документов по организации работ по защите персональных данных в администрации области".

Понятия и определения

персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

автоматизированные системы (АС) ИСПДн - программное обеспечение позволяющее производить автоматизированную обработку персональных данных;

администратор информационной безопасности (администратор) - сотрудник Управления, назначенный приказом и отвечающий за обеспечение информационной безопасности при работе с АС;

пользователь - сотрудник Управления, назначенный приказом и отвечающий за обработку ПДн в АС.

Методы взлома паролей

К одному из наиболее распространенных методов атаки на любую АС относится взлом паролей пользователей, которые проходят проверку подлинности для того чтобы можно было получить доступ к внутренней сети. Соответственно, если злоумышленник получит доступ к учетной записи пользователя, у него будет возможность получить доступ к внутренним документам Управления и к прочей защищенной информации. Помимо учетных записей пользователей для доступа к внутренней сети, также часто злоумышленники стараются взламывать аккаунты электронной почты, социальных сетей, блогов и прочего. Поэтому пользователям следует строго соблюдать меры по парольной защите.

Логическое угадывание

Этот метод является самым простым, и начинают обычно именно с логического угадывания пароля. Например, злоумышленник может попробовать угадать пароль пользователей, зная имя, фамилию и его год рождения, а его пароль состоит из «Фамилия + год рождения» или логин, указанный в обратном порядке, то такой пароль будет взломан через несколько минут.

Перебор паролей по словарю

Так как часто в качестве паролей используют одно слово, например название вулкана или другое «простое» слово и, максимум, добавляют к такому паролю одну цифру, злоумышленники могут взломать пароль, используя заранее отобранные пароли, которые загружаются из специальных словарей. В такие словари обычно включаются слова из разных языков, которые могут использовать неопытные или безразличные к своей безопасности пользователи. Подбор пароля, используя данный метод, обычно не занимает много времени и злоумышленник сможет получить доступ к учетной записи пользователя буквально через несколько часов.

Другим методом, связанным с перебором по словарю, называется перебор по таблице хешированных паролей. Этот метод используется тогда, когда злоумышленник смог определить хеши паролей и ему остается лишь найти в базе данных пароль, который будет полностью соответствовать данному хешу.

Метод грубой силы

Метод грубой силы или полный (прямой) перебор отличается от предыдущего метода тем, что при подборе пароля используется не определённый словарь, согласно которому можно подобрать простой пароль, а большое количество любых возможных комбинаций. В этом случае, все зависит лишь от сложности пароля и количества символов. В следующей таблице, можно приблизительно оценить сложность создаваемых паролей, если учесть что в паролях будут только лишь буквы одного регистра с цифрами и скорость перебора составляет 100000 паролей за одну секунду:

Количество знаков	**Количество вариантов**	**Время перебора**
1	36	менее секунды
2	1296	менее секунды
3	46 656	менее секунды
4	1 679 616	17 секунд
5	60 466 176	10 минут
6	2 176 782 336	6 часов
7	78 364 164 096	9 дней
8	2,821 109 9?1012	11 месяцев
9	1,015 599 5?1014	32 года
10	3,656 158 4?1015	1 162 года
11	1,316 217 0?1017	41 823 года
12	4,738 381 3?1018	1 505 615 лет

Соответственно, более-менее стойким паролем можно считать пароль, длина которого будет состоять не менее чем из восьми символов.

Использование человеческого фактора

Несмотря на то, что при использовании человеческого фактора не применяется какая либо технология, этот метод в большинстве случаев считается самым действенным и иногда даже самым быстрым, так как в этом случае злоумышленники получают пароли незаконным методом от самих пользователей, причем, последние об этом могут даже не подозревать. Прежде всего, при использовании этого метода получения пользовательских паролей

злоумышленник обычно узнает имена сотрудников организации, которые он может, как знать изначально, так и найти на том же, скажем, веб-сайте компании, а уже после этого, согласно продуманному заранее сценарию злоумышленник может получить от пользователей практически любые данные. Методов получения пользовательских паролей, используя человеческий фактор, очень много.

Основные способы следующие:

·***Фишинг***. Является довольно распространенным методом получения от пользователей необходимой информации. Сама атака происходит следующим образом: пользователю на почтовый ящик приходит письмо, в котором пользователю предлагают, перейдя по предоставленной ссылке, в целях обеспечения безопасности сменить на сайте свой пароль. На самом деле, такая ссылка ведет на сайт хакера со страницей, которая очень похожа на страницу официального сайта и при попытке смены своего пароля, пароль будет отправлен злоумышленнику;

·***Заражение компьютеров средствами «троянских коней»***. «Троянским конем» называется вредоносная программа, которая распространяется злоумышленниками, при помощи которой он может получить доступ данным, в зависимости от того, какую он поставил перед собой задачу. В свою очередь, пользовательские пароли не являются исключениями;

·***Кви про кво***. Данный метод обозначает недоразумение, возникшее в результате того, что одно лицо, вещь или понятие принято за другое. В случае с хищением паролей, этот способ подразумевает звонок злоумышленников. Злоумышленник может представиться техническим специалистом и узнать о уязвимостях, которые могут быть в организации и воспользоваться ими. Или же просто узнать пользовательский пароль по телефону;

·***Претекстинг***. Этот способ самый простой. Используя данный метод хищения пароля, злоумышленником выполняются действия, отработанные по заранее составленному сценарию. Он может начать общаться с пользователем на каком-то веб-сайте, средствами переписки по электронной почте и т.д. По вполне понятным причинам, данный метод может занять значительно больше времени, чем все указанные раньше.

Правила формирования паролей

Минимальные требования к сложности пароля:

• Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть или включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (LAN, USER и т.п.);

• Пароль должен состоять не менее чем из 8 (восьми) символов;

• В пароле должны присутствовать символы трех категорий из числа следующих четырех:

1. прописные буквы английского алфавита от A до Z;
2. строчные буквы английского алфавита от a до z;
3. десятичные цифры (от 0 до 9);
4. неалфавитные символы (например, !, $, #, %)

В целях обеспечения информационной безопасности и противодействия попыткам подбора, символы вводимого пароля не должны отображаться на экране в явном виде.

Пароли для пользовательских учетных записей должны соответствовать требованиям:

- Формирование и выдачу паролей для работы с АС рекомендуется осуществлять администратором;
- Максимальный срок действия пароля должен быть ограничен и должен меняться не реже 1 раза в 6 месяцев.
- Учетная запись пользователя, не сменившего вовремя пароль, должна автоматически блокироваться. Блокировка должна сниматься «вручную» администратором или специалистом службы технической поддержки с одновременной сменой пароля пользователя.
- Новый пароль пользователя не должен совпадать как минимум с тремя предыдущими паролями.
- Пароль не должен совпадать с именем учетной записи пользователя.
- В журнал учета работ АС должно заноситься сообщение о многократно не удавшихся попытках авторизации пользователя.
- Пароли пользователей на доступ к различным ресурсам должны быть разными.
- Недопустимо хранение пароля в открытом виде на любых видах носителей информации.

Пароли для административных учетных записей должны соответствовать требованиям:

- Максимальный срок действия пароля должен быть ограничен одним месяцем.
- Новый пароль администратора не должен совпадать как минимум с предыдущим паролем.
- Пароль не должен совпадать с именем учетной записи администратора.
- В случае не удавшейся попытки авторизации в журнал учета работ АС должно заноситься соответствующее сообщение. При многократных не удавшихся попытках авторизации должно генерироваться предупреждение системы обнаружения вторжений.
- Пароли на доступ к различным ресурсам должны различаться, не допускается использование универсальных паролей для административных учетных записей.
- Криптографические ключи, используемые для аутентификации, должны быть защищены парольными фразами. Требования к стойкости парольных фраз криптографических ключей идентичны требованиям к паролям административных учетных записей.

Порядок ввода пароля.

Непосредственно перед вводом пароля для предотвращения возможности неверного ввода пользователь должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPSLOCK (если это необходимо), а также проконтролировать расположение клавиатуры (клавиатура должна располагаться таким образом, что бы исключить возможность увидеть набираемый текст посторонними).

При вводе пароля пользователю запрещается проговаривать вслух вводимые символы.

Хранение паролей.

Недопустимо хранение пароля в открытом виде на любых видах носителей информации.

Журнал выдачи паролей пользователю должен храниться в надежно запираемом сейфе администратора.

Порядок выдачи (смены) пароля.

Новый пароль должен выдаваться пользователю только после обязательной регистрации в журнале выдачи паролей (приложение к Политике).

В случае выдачи пароля на бумажном носителе (для первоначального запоминания) в журнале выдачи паролей указывается регистрационный номер носителя, при этом на самом носителе указываются только регистрационный номер и пароль (обезличивание пароля).

При возникновении служебной необходимости в срочном доступе к АС временно отсутствующего пользователя разрешается произвести смену пароля пользователя администратором или лицом, курирующим вопросы организации защиты информационных систем ПДн, при этом должен быть составлен акт о смене пароля.

В случае возникновения необходимости в смене пароля в виду компрометации пользователь должен немедленно известить администратора или лицо, курирующее вопросы организации защиты информационных систем ПДн.

Внеплановая смена пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, перевод в другое структурное подразделение и т.п.) должна производиться непосредственно после окончания последнего сеанса работы данного пользователя.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, перевод в другое структурное подразделение и другие обстоятельства) администратора.

Сотрудники Техподдержки АС в течение суток после смены паролей должны передать на хранение их новые значения вместе с именами соответствующих учетных записей в запечатанном конверте администратору или лицу, курирующему вопросы организации защиты информационных систем ПДн. При получении конверта с новыми паролями старые пароли уничтожается с составлением соответствующего акта.

Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться администратором с момента получения письменного уведомления от кадрового подразделения.

Удаление учетных записей пользователей, уволенных или переведенных в другое структурное подразделение должно производиться администратором немедленно с момента получения письменного уведомления из кадрового подразделения.

Кадровое подразделение должно известить администратора о состоявшемся приказе в течение 24 часов после увольнения, перевода работника в другое структурное подразделение.

Ответственность при организации парольной защиты

Пользователю запрещается разглашать или передавать свой пароль для ввода другим лицам.

Администратору запрещается разглашать все известные ему имена учетный записей пользователей и их пароли или передавать журнал выдачи паролей другому сотруднику.

За разглашение парольной информации, сотрудник привлекается к ответственности в соответствии с действующим законодательством Российской Федерации.

Повседневный контроль действий пользователей АС при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора, периодический контроль возлагается на лицо, курирующее вопросы организации защиты информационных систем персональных данных или сотрудников службы Техподдержки данных АС.

Сотрудники и работники Управления должны быть ознакомлены с данной политикой под роспись.

ПРИЛОЖЕНИЕ
к политике парольной защиты

Журнал выдачи (смены) паролей

№ п/п	Ресистр. номер пароля (для бум.носителя)	Учетная запись			Дата выдачи	пользователь		Дата сдачи	Роспись администратора	Акт об уничтожении	
		АС	логин	пароль (не менее 8 символов)		ФИО	роспись			№	дата