Копия верна

Проректор по цифровому развитию

М.А. Фоменко

ПРИЛОЖЕНИЕ № 3

УТВЕРЖДЕНО
приказом ФГБОУ ВО «Кубанский государственный университет»
от 12 декабря 2019 года № 2300

ПОЛИТИКА
использования аутентификационной информации при доступе к информационным активам ФГБОУ ВО «Кубанский государственный университет»

1. Общие положения

1.1. Политика использования аутентификационной информации при доступе к информационным активам Федерального государственного бюджетного образовательного учреждения высшего образования (далее – ФГБОУ ВО) «Кубанский государственный университет» (далее – Политика) определяет требования к комплексу мер по использованию аутентификационной информации при реализации доступа к автоматизированным рабочим местам пользователей (далее – АРМ), серверам, активному сетевому оборудованию и средствам защиты информации ФГБОУ ВО «Кубанский государственный университет» (далее – Университет).

1.2. В общем случае под информационными активами понимаются:

информационные ресурсы, содержание защищаемую информацию (в базах данных, в файловом виде в каталогах).

информационные системы, в которых осуществляется обработка защищаемой информации, в совокупности со средствами обработки такой информации и с учетом технологии ее обработки.

1.3. Под аутентификационной информацией понимается информация, используемая пользователями и администраторами информационных активов для доступа к ним (имя пользователя, пароль, средства дополнительной аутентификации).

1.4. Настоящая Политика разработана в соответствии с:

приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

2. Порядок формирования и использования аутентификационной информации

2.1. Для обеспечения возможности однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами каждому пользователю формируется имя пользователя.

2.2. Для обеспечения возможности однозначного сопоставления устройства доступа на АРМ пользователя с информационными активами, к которым осуществляется доступ (объектами доступа), его имя должно соответствовать имени пользователя.

2.3. Имя пользователя и имя АРМ пользователя должны отождествляться с именем и фамилией пользователя, например, «i.ivanov» (при наличии технической возможности). В случае совпадения имён и фамилий у разных пользователей в наименование учётной записи должны быть добавлены дополнительные символы (например, буква отчества или цифра).

2.4. В случае привлечения третьих лиц для выполнения работ по настройке и тестированию информационных активов, им предоставляются временные учётные записи с предустановленным сроком их действия (при наличии технической возможности), доступ к которым блокируется по завершению работ.

2.5. При создании учётной записи должен быть задан тип учётной записи (при наличии технической возможности). Под типами учётных записей понимается: учётная запись пользователя, учётная запись администратора, временная учётная запись, системная учётная запись.

2.6. Использование гостевых учётных записей запрещено.

2.7. Локальная учётная запись администратора операционной системы Windows (Administrator) предназначена только для служебного использования администратором при настройке систем и не может быть использована для повседневной работы.

2.8. Учётные записи пользователей блокируются и подлежат удалению в системе по решению Администратора ИБ.

2.9. Сотрудники обязаны хранить в секрете персональные пароли доступа к информационным активам и не передавать их другим лицам. Передача личного пароля пользователя третьим лицам возможно только в случаях, регламентированных в пункте 2.10 настоящей Политики.

2.10. В случае необходимости при проведении проверочных мероприятий (внутренний аналитический аудит), которые требуют знания пароля пользователя, допускается раскрытие значений своего пароля проверяющему сотруднику. По окончанию проверочных работ сотрудники самостоятельно производят немедленную смену значений «раскрытых» паролей.

2.11. В случае возникновении нештатных ситуаций, форсмажорных обстоятельств, а также технологической необходимости использования имён и паролей сотрудников (в их отсутствие) допускается изменение паролей

администратором данного информационного актива.

Сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения в соответствии с требованиями настоящей Политики.

2.12. Хранение сотрудником (администратором, пользователем) аутентификационной информации допускается только в личном запираемом шкафу (ящике) либо в сейфе (запираемом шкафу, ящике) администратора соответствующей ИС.

2.13. При доступе к средствам обработки информации (серверам, активному сетевому оборудованию, средствам защиты информации) запрещается использование аутентификационной информации, заданной производителем «по умолчанию».

2.14. После получения доступа к информационному активу пользователь при первом входе в систему должен сменить пароль доступа (в случае наличия технической возможности), на пароль, удовлетворяющий требованиям настоящей Политики.

2.15. При вводе аутентификационной информации (пароля) должно обеспечиваться исключение отображения вводимой парольной информации (например, осуществляется замена вводимых символов условными знаками «-», «*» или иными знаками), при технической возможности реализации данного требования.

2.16. Запрещается передача аутентификационной информации пользователям при помощи почтовых сообщений, либо по иным открытым каналам связи.

2.17. В случае компрометации аутентификационных данных сотрудники должны сообщить об этом событии администратору информационной безопасности (далее – Администратор ИБ).

2.18. Предусматривается периодическая плановая (в соответствии с установленным сроком) и внеплановая смена паролей.

2.19. Внеплановая смена пароля обязательна в случае его компрометации. Также, внеплановая смена пароля и (или) блокирование учётной записи пользователя производится в случае прекращения его полномочий, непосредственно после окончания последнего сеанса работы данного пользователя.

2.20. Должностным лицам запрещается разглашать пароли, ставшие известными им в ходе служебной деятельности по обеспечению функционирования информационных систем.

3. Требования к качеству аутентификационной информации и мер по обеспечению её безопасности

3.1. К аутентификационной информации пользователей и администраторов информационных активов определены следующие требования представленные в таблице 1:

Таблица 1 – Требования к аутентификационной информации

№ п/п	Параметр качества пароля	Администратор	Пользователь
1	2	3	4
1	Минимальная длина пароля в символах	12	9
2	Максимальная длина пароля в символах	не ограничена	не ограничена
3	Содержание в пароле букв верхнего и нижнего регистра	да	да
4	Содержание в пароле специальных символов (@, #, $, &, * и тому подобное) и цифр (при наличии технической возможности)	обязательно	рекомендуется
5	Содержание в пароле личных имён, фамилий, кличек домашних животных, номеров телефонов, дат рождения, географических названий, именований АРМ и тому подобное.	запрещено	запрещено
6	Содержание в пароле общепринятых сокращений (Admin, Administrator, ViPNet, Cisco, User, UserID и так далее)	запрещено	запрещено
7	Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки	5	10
8	Блокировка сеанса доступа в информационную систему после времени бездействия (неактивности) пользователя (минут)	5	10
9	Блокировка программно-технического средства или учётной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации	20	10
10	Блокировка учётной записи после периода неиспользования (дней)	60	90
11	Минимальное отличие нового пароля от предыдущего (в позициях)	4	3
12	Количество уникальных паролей, устанавливаемых подряд (в течение установленного срока смены паролей)	не менее 5	не менее 3
13	Максимальный срок действия пароля	90 дней	120 дней
14	Минимальный срок действия пароля	нет	нет

3.2. Для простоты запоминания могут быть использованы парольные фразы, разделенные спецсимволами и цифрами.

3.3. 2.4. Пароль не должен совпадать с логином пользователя (наименованием учетной записи) и содержать легко угадываемые слова и числа (имена, даты рождения, номера документов и т.п.).

4. Ответственность за исполнение положений настоящей Политики

4.1. Ответственность за исполнение положений настоящей Политики возлагается на всех сотрудников Университета, осуществляющих работу на средствах вычислительной техники.

4.2. Пользователи информационных активов Университета должны:

в случае самостоятельного формирования пароля доступа к компонентам информационных активов руководствоваться требованиями к качеству аутентификационной информации и мер по обеспечению её безопасности, установленными положениями настоящей Политики;

в случае получения аутентификационной информации от администратора информационного активов осуществить смену пароля пользователя при наличии технической возможности, а в случае отсутствия технической возможности обеспечить условия его сохранности;

следить за сроком действия паролей и своевременно производить их смену, а в случае отсутствия технической возможности обращаться по вопросу их смены к администраторам информационных активов;

не допускать многократного ввода неправильного пароля и блокировки своих учётных записей;

в случае компрометации аутентификационной информации уведомлять Администратора ИБ.

4.3. Администратор ИС Университета обязан:

создавать учётные записи пользователей и обеспечивать управление их жизненным циклом в соответствии с требованиями к качеству аутентификационной информации и мерами по обеспечению её безопасности, установленными положениями настоящей Политики;

своевременно осуществлять блокировку/разблокировку учётной записи пользователя, а также внеплановую смену пароля в случае запросов пользователей (с информированием Администратора ИБ об инциденте информационной безопасности).

5. Администратор ИБ обязан:

руководствоваться положениями настоящей Политики при задании аутентификационной информации на доступ к средствам защиты информации;

устанавливать требования к качеству аутентификационной информации и мерам по обеспечению её безопасности в соответствии с требованиями, установленными положениями настоящей Политики;

управлять (создавать, изменять, удалять, блокировать, разблокировать) учётными записями пользователей, зарегистрированных в подсистеме

управления доступом средства защиты информации от несанкционированного доступа (при его наличии);

осуществлять планирование и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики структурными подразделениями Университета;

5.1. Лица, виновные в нарушении положений настоящей Политики, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой и административной ответственности.