УТВЕРЖДАЮ
ФГБОУ ВПО «НВГУ»
_____ С.И. Горлов
«30» _____ 2013 г.

Инструкция пользователя информационной системы персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана на основании:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации №781 от 17 ноября 2007г.;
- Приказа №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного ФСТЭК России от 05.02.2010 г.;
- Приказа №1640 от «27» мая 2010г. «Об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Ректором ФГБОУ ВПО «НВГУ»;
- Положения «О разрешительной системе допуска пользователей к обрабатываемой в ИСПДн информации», утвержденного Ректором ФГБОУ ВПО «НВГУ» от «30» мая 2013 г.

1.2. Данная инструкция определяет общие обязанности, права и ответственность пользователя информационной системы персональных данных (далее – ИСПДн) ФГБОУ ВПО «НВГУ» (далее - НВГУ) по обеспечению информационной безопасности при работе со сведениями конфиденциального характера.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник НВГУ, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Обязанности пользователя

2.1. При выполнении работ в ИСПДн Пользователь обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн, правила работы и порядок регистрации в ИСПДн, доступа к информационным ресурсам ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (АРМ);
- хранить в тайне свои идентификационные данные (имена, пароли и т.д.);
- выполнять требования «Инструкции по парольной защите в информационной системе персональных данных», предъявляемые к парольной системе (нормативы на длину, состав, периодичность смены пароля и т.д.), осуществлять вход в ИСПДн только под своими идентификационными данными;
- передавать для хранения установленным порядком свое индивидуальное устройство идентификации, личную ключевую дискету и другие реквизиты разграничения доступа, только руководителю своего подразделения или администратору безопасности ИСПДн (ответственному за информационную безопасность подразделения);
- выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей ИСПДн;
- немедленно вызывать администратора безопасности ИСПДн (ответственного за безопасность информации в подразделении) и ставить в известность руководителя подразделения в случае утери персональной ключевой дискеты, индивидуального устройства идентификации или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной АРМ, несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ ставить в известность администратора безопасности ИСПДн (ответственного за безопасность информации в подразделении) при необходимости внесения изменения в состав аппаратных и программных средств АРМ;
- работать в ИСПДн только в разрешенный период времени;

- немедленно выполнять предписания администраторов безопасности ИСПДн, предоставлять свое АРМ администратору безопасности для контроля;
- ставить в известность администраторов ИСПДн в случае появления сведений или подозрений о фактах НСД к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;
- уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;
- сообщать руководителю своего подразделения обо всех проблемах, связанных с эксплуатацией ИСПДн.

2.2. Пользователю категорически ЗАПРЕЩАЕТСЯ:

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИСПДн (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формуляром АРМ;
- осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.), в том числе для временного хранения;
- оставлять включенное без присмотра свое АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);
- передавать кому-либо свое индивидуальное устройство идентификации (персональную ключевую дискету) в нарушение установленного порядка, делать неучтенные копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИСПДн (в том числе средств

защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора безопасности ИСПДн (ответственного за безопасность информации) и руководителя своего подразделения;

- подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;
- осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;
- фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;
- разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;
- вносить изменения в файлы, принадлежащие другим пользователям.

3. Права пользователя

Пользователь имеет право:

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными;
- своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей;
- требовать от администратора безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Ответственность пользователя

4.1. Пользователь несет персональную ответственность за:

- ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, и целостность установленного программного обеспечения.
- разглашение сведений, отнесенных к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы;
- нарушение функционирования ИСПДн, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

4.2. Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами НВГУ (см. Приложение № 1).

Приложение № 1. Выдержки из статей Уголовного кодекса РФ, определяющие ответственность пользователей за нарушение установленных правил обработки информации

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Комментарий к статье 272

1. Понятие компьютерной информации определено в комментируемой статье. Предметом компьютерной информации являются информационные ресурсы, которые в ст. 2 Федерального закона от 20 февраля 1995 г. "Об информации, информатизации и защите информации" рассматриваются как отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в частности в банках данных. Эти ресурсы согласно ст. 2 Закона содержат сведения о лицах, предметах, событиях, процессах, населении независимо от формы их представления. В законе далее дается полная расшифровка их содержания.

2. Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать самовольное получение информации без разрешения ее собственника или владельца. В связи с тем, что речь идет об охраняемой законом информации, неправомерность доступа к ней потребителя характеризуется еще и нарушением установленного порядка доступа к этой информации. Если нарушен установленный порядок доступа к охраняемой законом информации, согласие ее собственника или владельца не исключает, по нашему мнению, неправомерности доступа к ней.

Собственником информационных ресурсов, информационных систем, технологии и средств их обеспечения является субъект, в полном объеме

реализующий права владения, пользования, распоряжения указанными объектами.

Владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения является субъект, осуществляющий владение и пользование указанными объектами и реализующий права распоряжения в пределах, установленных законом.

Пользователем (потребителем) информации является субъект, обращающийся к информации (подробнее о собственниках, владельцах и пользователях компьютерной информации см. Федеральный закон от 20 февраля 1995 г.).

3. Способы неправомерного доступа к компьютерной информации могут быть самыми различными, например, представление фиктивных документов на право доступа к информации, изменение кода или адреса технического устройства, нарушение средств или системы защиты информации, кража носителя информации.

4. Ответственность по ст. 272 УК наступает в том случае, если деяние повлекло указанные в ч. 1 этой статьи последствия.

Под уничтожением информации следует понимать ее утрату при невозможности ее восстановления.

Блокирование информации - это невозможность ее использования при сохранности такой информации.

Модификация информации означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя.

Под копированием информации следует понимать ее переписывание, а также иное тиражирование при сохранении оригинала. Представляется, что копирование может означать и ее разглашение.

Нарушение работы ЭВМ, системы ЭВМ или их сети может выразиться в их произвольном отключении, в отказе выдать информацию, в выдаче искаженной информации при сохранении целости ЭВМ, системы ЭВМ или их сети.

5. Неправомерный доступ к компьютерной информации считается оконченным с момента наступления в результате этого неправомерного доступа к ней одного или нескольких из упомянутых последствий.

6. Представляется, что к лицам, как указывается в ч. 2 ст. 272 УК, "равно имеющим доступ" к ЭВМ, системе ЭВМ или их сети, положение ч. 1 этой статьи о несанкционированном доступе к компьютерной информации относится в тех случаях, когда они вышли за пределы определенных им обязанностей по работе и вторглись в ту сферу компьютерной информации, на которую их обязанности не распространяются. Полагается, что о других случаях несанкционированного доступа к компьютерной информации для лиц, уже имеющих доступ, говорить вряд ли можно.

7. С субъективной стороны преступление может быть совершено только с прямым умыслом. Мотивами преступления могут быть корыстные или хулиганские побуждения, месть, зависть и др.

8. Субъектом преступления, предусмотренного ч. 1 ст. 272 УК, а также при совершении его группой лиц могут быть любые лица, достигшие 16 лет. При совершении преступления, предусмотренного ч. 2 этой статьи, при других обстоятельствах, субъектами могут быть лишь лица, занимающие определенное служебное положение или имеющие доступ к ЭВМ, системе ЭВМ или их сети, т. е. субъект специальный.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Комментарий к статье 273

1. В ст. 273 УК речь идет о разработке и распространении компьютерных вирусов путем создания программ для ЭВМ или внесения изменений в существующие программы.

Опасность компьютерного вируса состоит в том, что он может привести, к полной дезорганизации системы компьютерной информации.

2. Именно высокой степенью общественной опасности объясняется то, что уголовный закон преследует достаточно строго за сам факт создания программ для ЭВМ или внесения изменений в существующие программы, не оговаривая наступление каких-либо последствий.

3. Преступление, предусмотренное ст. 273 УК, считается оконченным, когда программа создана или внесены изменения в существующую программу, независимо от того, была ли она использована или распространена.

4. О заведомости для виновного возможных последствий при создании вредоносных программ или внесении изменений в существующие программы см., например, комментарии к ст. 63 и 105 УК.

5. Об уничтожении, блокировании, модификации либо копировании информации, нарушении работы ЭВМ, системы ЭВМ или их сети см. комментарий к ст. 272 УК.

6. Под использованием либо распространением вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в ЭВМ, систему ЭВМ или их сеть, а также продажа, обмен, дарение или безвозмездная передача другим лицам.

7. Представляется, что под распространением вредоносных программ следует понимать и их копирование (см. комментарий к ст. 272 УК).

8. С субъективной стороны преступление может быть совершено как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям. При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели, которую перед собой ставил виновный, а когда наступили последствия, к достижению которых он стремился, - и в зависимости от наступивших последствий. В этом случае действия, предусмотренные ст. 273 УК, оказываются лишь способом достижения поставленной цели. Совершенное деяние подлежит квалификации по совокупности совершенных преступлений.

9. К тяжким последствиям, наступившим по неосторожности (ч. 2), могут быть отнесены, например, гибель людей, причинение вреда их здоровью, дезорганизация производства на предприятии или в отрасли промышленности, осложнение дипломатических отношений с другим государством, возникновение вооруженного конфликта. При этом необходимо иметь в виду, что наступившие последствия могут привести и к необходимости квалификации данного преступления по совокупности с другими преступлениями в зависимости от характера последствий и отнесения заведомо к легкомыслию или к косвенному умыслу в виде безразличного отношения к последствиям.

10. Субъектом преступления может быть любое лицо, достигшее 16 лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Комментарий к статье 274

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит в несоблюдении правил режима их работы, предусмотренных инструкциями, исходящими из их технических характеристик, правил внутреннего распорядка, а также правил обращения с компьютерной

информацией, установленных собственником или владельцем информации либо законом или иным нормативным актом.

2. Под охраняемой законом информацией следует понимать информацию, изъятую из публичного (открытого) оборота на основании закона, других нормативных (включая ведомственные) актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По общему правилу такая информация имеет гриф ограниченного пользования.

Представляется, что частные фирмы, включая коммерческие банки, вправе устанавливать ограничительные грифы в целях сохранения коммерческой или банковской тайны.

3. Для наступления ответственности по ст. 274 УК необходимо установить, что упомянутое нарушение правил эксплуатации повлекло уничтожение, блокирование или модификацию охраняемой законом информации при условии причинения существенного ущерба. Об уничтожении, блокировании или модификации компьютерной информации см. комментарий к ст. 272 УК.

Что касается существенности ущерба, причиненного нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, то это оценочное понятие, которое зависит в каждом конкретном случае от многих показателей, относящихся к применяемым техническим средствам (ЭВМ и др.), к содержанию информации, степени повреждения и многим другим показателям, которые должны оцениваться следователем и судом. Во всяком случае, существенный вред должен быть менее значительным, чем причинение тяжких последствий, о которых говорится в ч. 2 данной статьи.

4. С субъективной стороны преступление может быть совершено по неосторожности в виде, как небрежности, так и легкомыслия. При установлении умысла на нарушение правил эксплуатации ЭВМ, системы ЭВМ и их сети деяние, предусмотренное ст. 274 УК, становится лишь способом совершения преступления. Преступление в этом случае подлежит квалификации по наступившим последствиям, которые предвидел виновный, по совокупности с преступлением, предусмотренным данной статьей УК.

5. Субъект преступления специальный - лицо, имеющее доступ к эксплуатации упомянутых технических средств. Это могут быть программисты, операторы ЭВМ, техники-наладчики, другие лица, по работе имеющие к ним доступ.

О тяжких последствиях, наступивших по неосторожности, см. комментарий к ст. 273 УК.

Статья 293. Халатность

1. Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом

интересов общества или государства, - наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.

2. То же деяние, повлекшее по неосторожности смерть человека или иные тяжкие последствия, наказывается лишением свободы на срок до пяти лет.

Комментарий к Статье 293

1. Своеобразие данного состава преступления заключается в том, что содержащиеся в диспозиции ст. 293 УК признаки относятся как к объективной стороне халатности, так и к ее субъективной стороне.

Неисполнение должностным лицом своих обязанностей означает его бездействие, характеризующееся непринятием мер по службе, несовершением конкретных действий, входящих в круг полномочий указанного лица.

Под ненадлежащим исполнением обязанностей понимается совершение должностным лицом действий не в полном объеме либо вопреки установленному порядку или правилам.

2. Уголовно наказуемая халатность предполагает в обязательном порядке, что исполнение соответствующих обязанностей входило в круг правомочий должностного лица, закрепленных в конкретном законе либо ином нормативном правовом акте, а также в соответствующих должностных инструкциях, приказах, распоряжениях и т.д. Отсутствие надлежаще оформленного правового акта о круге обязанностей должностного лица исключает ответственность за халатность.

При решении вопроса об ответственности должностного лица за совершение данного преступления необходимо устанавливать, какие конкретно обязанности не были исполнены либо исполнены им ненадлежаще и имелась ли у него реальная возможность исполнить их должным образом. В случае, когда такая возможность отсутствовала, ответственность по ст. 293 УК исключается.

3. Состав рассматриваемого преступления имеется лишь в случае, когда по делу установлена причинная связь между противоправными действиями (бездействием) должностного лица и наступившими последствиями. Отсутствие такой связи исключает ответственность по ст. 293 УК (например, в случае, когда материальные ценности на складе либо в ином хранилище государственного или муниципального учреждения уничтожены ввиду стихийного бедствия).

4. Субъективная сторона рассматриваемого преступления выражается в недобросовестном или небрежном отношении к службе.

Если отношение должностного лица к неисполнению или ненадлежащему исполнению своих обязанностей характеризуется недобросовестностью, то в этом случае отношение указанного лица к последствиям деяния выражается в

форме легкомыслия, т.е. когда это лицо без достаточных к тому оснований самонадеянно рассчитывает на предотвращение вредных последствий деяния.

Если же отношение должностного лица к неисполнению или ненадлежащему исполнению своих обязанностей характеризуется небрежностью, то отношение его к последствиям преступления может выражаться только в форме небрежности.

5. Последствия рассматриваемого состава преступления в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства аналогичны последствиям от иных должностных преступлений.

6. Данное преступление признается имеющим квалифицирующие признаки, если оно повлекло по неосторожности смерть человека или иные тяжкие последствия (ч. 2 ст. 293 УК). В случае, когда таковые наступают не в результате неисполнения либо ненадлежащего исполнения должностным лицом своих обязанностей, а вследствие профессионального упущения либо ошибки (например, смерть больного наступила ввиду допущенной врачом-хирургом ошибки в диагнозе), содеянное не может быть квалифицировано как халатность (Сборник постановлений и определений по уголовным делам Верховного Суда РСФСР. 1981-1988 гг. С. 257-258). Однако, если указанные последствия наступили в результате неисполнения или ненадлежащего исполнения должностным лицом своих обязанностей (например, смерть человека наступила вследствие неоказания немедленной медицинской помощи из-за отказа дежурного врача больницы госпитализировать больного), действия его подпадают под признаки преступления, предусмотренного ст. 293 УК.