



УТВЕРЖДАЮ
Заместитель директора
ИНХ СО РАН, д.х.н.

Д.Н. Дыбцев

« 03 » октября 2024 г.

**Инструкция по основам обеспечения информационной безопасности
при работе в сети Интернет и
локальной вычислительной сети ИНХ СО РАН**
(рекомендовано Министерством науки и высшего образования Российской Федерации)

Цель инструкции: довести до пользователей основы Информационной безопасности при работе в сети Интернет и локальной вычислительной сети ИНХ СО РАН для сокращения количества киберинцидентов.

Основные понятия

- **Информация** – сведения (сообщения, данные) независимо от формы их представления.
- **Несанкционированный доступ** – доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.
- **Пользователь** – это лицо (сотрудник Института), участвующее в процессах автоматизированной обработки информации в информационной системе Института и имеющее доступ к программному обеспечению и данным, обрабатываемым в этой системе.
- **Пароль** – средство проверки личности пользователя для доступа к ИС, обеспечивающее идентификацию (распознавание пользователя) и аутентификацию (процесс подтверждения права на доступ) на основе сведений, известных только пользователю.
- **Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
- **Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).
- **Служебная информация ограниченного распространения** – несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.
- **Электронная подпись** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (электронная подпись является гарантией того, что с момента отправки документа его содержание не изменялось).
- **Машинный носитель информации** – материальный носитель, используемый для записи, хранения и воспроизведения информации в электронном виде (flash-накопители, CD/DVD-диски и др.)

Обязанности пользователя при работе за компьютером

- Знать и строго соблюдать требования по работе с установленными программными средствами защиты информации.
- Не использовать «внешние» мессенджеры при выполнении служебных задач (Discord, Microsoft Teams, Skype for Business, Snapchat, Telegram, Threema, Viber, WhatsApp, WeChat).
- Активировать временную блокировку экрана (Win+L) в случае ухода от компьютера.
- Не осуществлять попыток отключения установленных на компьютере средств защиты информации.
- Разместить монитор на рабочем месте таким образом, чтобы исключить несанкционированный просмотр отображаемой информации.
- Не ремонтировать или не вносить какие-то изменения в аппаратную и программную конфигурацию компьютера самостоятельно.
- Не подключать сторонние устройства к рабочему компьютеру (мобильные телефоны, планшеты и пр.).
- Разграничить рабочие и личные пространства.
- Не допускать хранение личных данных на рабочих компьютерах.

Обязанности пользователя при работе с машинными носителями информации

- Обеспечивать физическую безопасность съемных носителей информации, используемых для выполнения функциональных обязанностей (в служебной деятельности).
- Запрещается использовать машинный носитель информации до окончания проверки антивирусным средством

Обязанности пользователя при работе с электронной подписью

- Обеспечить физическую безопасность электронной подписи (токена).
- В случае компрометации (утери, кражи) электронной подписи (токена) необходимо в кратчайшие сроки уведомить главного бухгалтера Института, курирующего выдачу электронной подписи (токена).
- Не передавать электронную подпись (токен) третьим лицам.

Правила использования паролей

- Использовать только свои персональные учетные записи (идентификаторы).
- Во время ввода пароля необходимо исключить возможность его просмотра посторонними лицами.
- Использовать надежные пароли:
 - ✓ Длина пароля должна быть не менее 6 символов.
 - ✓ Рекомендуемая смена пароля не реже 1 раза в квартал (3 месяца).
 - ✓ Не использовать в пароле комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 12345678, 123qwe, qwerty12345 и т.д.).
 - ✓ Не использовать в пароле собственные даты рождения и даты рождения своих близких, собственные имена и фамилии.
 - ✓ При смене пароля, новый пароль должен отличаться от старого не менее чем на 3 символа.
- При компрометации пароля, незамедлительно сменить его.
- Не хранить пароли в легко доступных местах (на мониторе, на обратной стороне клавиатуры и т.п.).
- Не хранить пароли на бумажном носителе (в блокнотах, ежедневниках, на отдельных листах бумаги).

- Не использовать функции сохранения пароля (автозаполнение) в формах аутентификации.
- Не использовать пароли доступа, заданные производителями оборудования и программного обеспечения, по умолчанию.
- Никому не сообщать свои пароли.
- Не использовать один и тот же пароль для разных информационных ресурсов.

Правила обеспечения антивирусной защиты информации

- Не отключать, не изменять настройки или не создавать препятствия для работы антивирусных средств.
- Не использовать при работе «зараженный» либо с подозрением на «заражение» носитель информации и/или файл.
- При обмене информацией использовать средства антивирусной защиты.
- При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) незамедлительно оповестить об этом структурное подразделение, ответственное за обеспечение информационной безопасности.

Обязанности пользователя при работе с электронной почтой и в сети Интернет

- Использовать доступ к сети Интернет исключительно для исполнения функциональных обязанностей (служебной деятельности).
- Не использовать сторонние средства для организации доступа к сети Интернет (по средствам использования мобильных телефонов, USB-модемы и т.д.).
- Не открывать вложения в сообщениях, содержащих исполняемые файлы (*.EXE, *.BAT, *.COM, *.MSI, *.SCR, *.CMD и др.).
- Не открывать вложения в сообщениях рекламного, развлекательного, оскорбительного характера.
- Не переходить по ссылкам на сайты из подозрительных электронных сообщений, в том числе сообщений, содержащих приглашения «открыть», «запустить», «посетить», «нажать», «перейти».
- Не отправлять электронные письма от имени других работников организации, если иное не определено их служебными обязанностями.
- Не предпринимать попытки несанкционированного доступа к почтовым ящикам других работников организации.
- Не использовать для обмена информацией, получаемой в ходе осуществления функциональных обязанностей (служебной деятельности), сторонние сайты и ресурсы, предоставляющие услуги хранения и обмена информацией (файлообменники).
- Не размещать (публиковать) информацию, получаемую в ходе осуществления функциональных обязанностей (служебной деятельности), на общедоступных ресурсах.

Защищаемая информация

Защищаемая информация, не содержащая сведений, составляющих государственную тайну, обрабатываемая в ИНХ СО РАН:

- **Персональные данные;**
- **Технологическая информация информационных систем;**
- **Парольная информация;**
- **Служебная информация ограниченного распространения.**

Обязанности пользователя при работе с защищаемой информацией

- **Хранить документы ограниченного распространения в строго определенных для этого помещениях (далее – Помещения).**
- **Уборку Помещений, производить в присутствии работников, ответственных за сохранность информации ограниченного распространения.**
- **Осуществлять автоматизированную обработку защищаемой информации исключительно на компьютерах, предназначенных для обработки такой информации.**
- **Не осуществлять фотографирование защищаемой информации (документов, экрана монитора и пр.).**
- **При выходе из Помещения (в течение рабочего дня / в конце рабочего дня) обеспечить невозможность несанкционированного доступа к документам, содержащим информацию ограниченного распространения (убирать документы со стола в запираемый ящик/сейф, блокировать компьютер).**

Об использовании информационных систем и (или) программ принадлежащих иностранным юридическим лицам и (или) иностранным гражданам

Запрещается использование принадлежащих иностранным юридическим лицам и (или) иностранным гражданам информационных систем и (или) программ для электронных вычислительных машин для:

- **передачи платежных документов,**
- **предоставления информации, содержащей персональные данные граждан Российской Федерации,**
- **предоставления информации, содержащей данные о переводах денежных средств в рамках применяемых форм безналичных расчетов, сведения, необходимые для осуществления платежей и (или) сведения о счетах (вкладах) граждан Российской Федерации в банках.**

ч. 8 ст. 10 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

"Перечень информационных систем и (или) программы для электронных вычислительных машин, указанных в ч. 8 ст. 10 Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (утв. Роскомнадзором):

- **Discord;**
- **Microsoft Teams;**
- **Skype for Business;**
- **Snapchat;**
- **Telegram;**
- **Threema;**
- **Viber;**
- **WhatsApp;**
- **WeChat.**

Ответственность пользователя за нарушение требований в области защиты информации

Ответственность

Пользователь информационных ресурсов (систем) несет ответственность за:

- **ненадлежащее исполнение или неисполнение своих функциональных обязанностей;**
- **разглашение защищаемой информации, ставшей известной ему в ходе выполнения функциональных обязанностей (служебной деятельности);**
- **нарушение функционирования информационных систем, уничтожение, блокирование, копирование, фальсификацию информации** (ответственность несет пользователь, под чьими идентификационными данными было совершено нарушение).

МЕРА ОТВЕТСТВЕННОСТИ УСТАНОВЛИВАЕТСЯ ПО ИТОГАМ СЛУЖЕБНОГО РАССЛЕДОВАНИЯ!

Административная (КоАП РФ):

ч.1 ст. 13.11 – обработка персональных данных в случаях, не предусмотренных законом.

Штраф на должностных лиц – до 20 тыс. руб., на юридических – до 100 тыс. руб.

ст. 13.14 – разглашение информации с ограниченным доступом.

Штраф на должностных лиц до 50 тыс. руб., на юридических – до 200 тыс. руб.

ст. 13.11.12 – незаконное использование принадлежащих иностранным юридическим лицам и ... информационных систем и (или) программ для электронных вычислительных машин

Штраф на должностных лиц от 30 тыс. руб. до 50 тыс. руб., на юридических – от 100 тыс. руб. до 700 тыс. руб..

Дисциплинарная (ТК РФ):

ст. 81 – Разглашение.

Штрафные санкции: увольнение.

ст. 192 – иные нарушения в области персональных данных.

Штрафные санкции: замечание или выговор.

Гражданско-правовая (ГК РФ):

ст. 15 – Причинение убытков.

Штрафные санкции: возмещение убытков.

ст. 151 – Причинение морального вреда.

Штрафные санкции: компенсация морального вреда.

Уголовная (УК РФ):

ч. 2 ст. 137 – незаконное собирание персональных данных с использованием служебного положения.

Штраф – до 400 тыс. руб., или лишение свободы на срок до четырех лет.

ст. 272 – неправомерный доступ к компьютерной информации.

Штрафные санкции: лишение свободы на срок до пяти лет.

Действия пользователя в случае нарушения требований информационной безопасности

Если Вы видите, что коллега, нарушает правила информационной безопасности – подойдите и скажите ему об этом!

При возникновении (предпосылок к возникновению) инцидентов в ИБ необходимо незамедлительно оповестить об этом своего руководителя подразделения и структурное подразделение, ответственное за обеспечение информационной безопасности, в ИНХ СО РАН Отдел развития информационных технологий (утрача носителей информации, компьютерные вирусы и пр.).

Нормативная база

- Федеральный закон от 27.07.2006 № 149-ФЗ «**Об информации, информационных технологиях и о защите информации**»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «**О персональных данных**»;
- Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «**Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности**»;
- Постановление Правительства Российской Федерации от 21.03.2012 № 211 «**Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами**»;
- Приказ Министерства науки и высшего образования Российской Федерации от 26.06.2018 № 8н «**Об обработке персональных данных в Министерстве науки и высшего образования Российской Федерации**»;
- Приказ Министерства науки и высшего образования Российской Федерации от 13.06.2023 № 598 «**Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве науки и высшего образования Российской Федерации и организациях, подведомственных Министерству науки и высшего образования Российской Федерации**» (Зарегистрирован 28.08.2023 № 74982).