



ГРИНАТОМ

Обучение пользователей правилам работы со средствами криптографической защиты информации

Программа обучения пользователей правилами работы с СКЗИ

✓ Понятие безопасности информации

✓ Типичные причины нарушений пользователей

✓ Требования к эксплуатации СКЗИ

✓ Правила работы с СКЗИ

✓ Меры предосторожности при работе с паролями

✓ Ответственность за нарушение правил



Корпоративные ценности ЗАО «Гринатом»

Корпоративные ценности компании - система принципов, на которых основывается ее деятельность, организация труда и стиль поведения сотрудников.

У компании «Гринатом» 6 ценностей:

- ✓ **Ответственность за результат**
- ✓ **Эффективность**
- ✓ **Уважение**
- ✓ **Безопасность**
- ✓ **Единая команда**
- ✓ **На шаг впереди**

Безопасность – наивысший приоритет. В нашей работе мы в первую очередь обеспечиваем полную безопасность людей и окружающей среды. В безопасности нет мелочей – мы знаем правила безопасности и выполняем их, пресекая нарушения. Особое внимание мы уделяем надежности/доступности сервисов и корпоративных информационных систем. Наши клиенты могут быть спокойны за сохранность их данных. Мы соблюдаем все внутренние регламенты и процедуры.



БЕЗОПАСНОСТЬ

это защищенность от возможного нанесения **ущерба** при возникновении различных возможных угроз

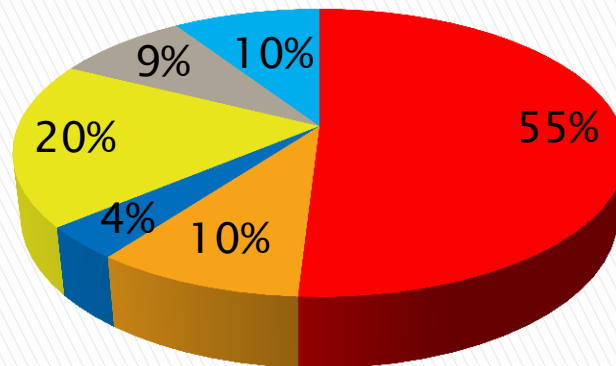


Ущерб может быть прямым и косвенным:

- ✓ материальный
- ✓ моральный
- ✓ физический

Субъектами нанесения ущерба, в конечном счете, всегда являются люди

Влияние осведомленности пользователей на уровень информационной безопасности

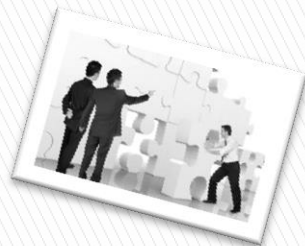


- Ошибки персонала
- Вирусы
- Обиженные сотрудники
- Нечестные сотрудники
- Проблемы электропитания
- Внешние нападения

Более 50 процентов от общего объема нарушений и преступлений составляют ошибки персонала



Обеспечение безопасности – задача всех работников организации



Пожарная безопасность обеспечивается не только пожарной дружиной, но и всеми сотрудниками, которые соблюдают установленные правила (не бросают окурки, не пользуются неисправленными электроприборами и т.п.).

Состояние безопасности предприятия (как информационной, так и пожарной) **зависит от каждого**

В состав системы обеспечения информационной безопасности входят все сотрудники, имеющие прямое или косвенное отношение к системе

Типичные причины нарушений пользователей

- ▶ Использование ресурсов не по назначению



Действие:

использование предоставленных сотрудникам аппаратно-программных средств ГК «Росатом» в личных (иных, кроме служебных) целях

Последствия:

потери из-за непроизводительного использования ресурсов АС и рабочего времени, создание помех и дополнительных угроз основным технологическим процессам

Контрмеры:

запрет или введение существенных ограничений на использование аппаратно-программных средств не по назначению (в личных целях)

Пользователь не имеет право использовать предоставленные ему ресурсы ГК «Росатом» в личных целях



Типичные причины нарушений пользователей

- ▶ Непринятие мер по предотвращению порчи или утраты оборудования

Действие:

неумышленная порча или принятие мер по предотвращению порчи или утраты (хищения) технических средств, носителей информации, повреждение линий связи...

Последствия:

прямой материальный ущерб. Частичный или полный отказ системы - потери из-за простоев и затраты на восстановление ресурсов и работоспособности (технологических процессов)

Контрмеры:

повышение ответственности за сохранность и физическую целостность аппаратных средств (материальная компенсация в пользу ГК «Росатом»)

Если пользователь оказался свидетелем порчи имущества ГК «Росатом» он должен незамедлительно сообщить о произошедшем непосредственному руководителю



Типичные причины нарушений пользователей

- ▶ Несанкционированное изменение конфигурации устройств и программ

Действие:

самовольное изменение состава и конфигурации используемых аппаратных и программных средств, отключение или изменение режимов работы оборудования и программ

Последствия:

частичный или полный отказ системы.
Потери из-за простоев и затраты на восстановление ресурсов и работоспособности (технологических процессов), внедрение «жучков»

Контрмеры:

введение запретов и повышение ответственности за физическую целостность аппаратно-программных ресурсов



Пользователю запрещается: вскрытие системного блока ЭВМ (для протирания пыли), мыши, клавиатуры, добавление в аппаратную часть ЭВМ дополнительных плат для увеличения производительности, инсталляция сторонних программ, внесение изменений в настройки аппаратной части ЭВМ, программных продуктов, установленных на ЭВМ.



Типичные причины нарушений пользователей

- ▶ Инсталляция и/или запуск сторонних программ на рабочих станциях

Действие:

несанкционированное внедрение и использование неразрешенных и сторонних программ, не имеющих отношения к производственной деятельности

Последствия:

необоснованный расход ресурсов системы (загрузка процессора, каналов связи, оперативной памяти и памяти на внешних носителях), возникновение конфликтов ПО, заражение компьютеров вирусами

Контрмеры:

запрет самостоятельной разработки, установки и использования неучтенных, не разрешенных программ (не относящихся к производственному процессу)



Типичные причины нарушений пользователей

- ▶ Отключение или создание помех для работы штатных антивирусных программ

Действие:


отключение или создание препятствий для работы антивирусных программ, неправильные действия в случае обнаружения вирусов

Последствия:

потери из-за заражения компьютера вирусами и распространение эпидемии на другие сервера и рабочие станции (потеря данных, компрометация конфиденциальных сведений, простой системы, затраты на восстановление)

Контрмеры:

повышение ответственности пользователей, внедрение более совершенных антивирусных средств



При обнаружении вирусного заражения ЭВМ пользователь обязан прекратить обработку информации на компьютере и сообщить о произошедшем в подразделение информационной безопасности, эксплуатирующей систему



Типичные причины нарушений пользователей

► Использование нелицензионного программного обеспечения

Действие:

использование нелицензионного программного обеспечения на компьютерах предприятий отрасли (пиратских копий программ)

Последствия:

судебные иски правообладателей на компенсацию ущерба, возбуждение уголовного дела по ст. 146 УК РФ «Нарушение авторских и смежных прав» и связанные с этим риски, потеря репутации, выход из строя ряда АС

Контрмеры:

повышение ответственности конечных пользователей и обслуживающего персонала, усиление контроля, применение средств создания замкнутой программной среды



Типичные причины нарушений пользователей

- ▶ Нарушение порядка формирования, использования, хранения и резервного копирования критичной информации

Действие:

непреднамеренное удаление или искажение программ и файлов с важной (не обязательно конфиденциальной) информацией, ввод ошибочных данных и т.п.

Последствия:

потери из-за простоев и затраты на восстановление ресурсов и работоспособности

Контрмеры:

упорядочение работы (наведение порядка), повышение ответственности исполнителей, внедрение процедур резервного копирования важных данных



Типичные причины нарушений пользователей

- ▶ Нарушение установленного порядка обращения с конфиденциальной информацией

Действие:

разглашение (в результате неосторожных действий) конфиденциальной информации, или предоставление к ней общего доступа (сохранение на незащищенных носителях, пересылка по ошибочному адресу и т.п.)

Последствия:

потери из-за утечки коммерческой тайны к конкурентам, потеря имиджа ГК «Росатом»

Контрмеры:

повышение ответственности исполнителей за соблюдение правил обращения с конфиденциальной информацией, внедрение специальных средств защиты

АДМИНИСТРАТИВНАЯ ст. 13.14 КоАП РФ

наложение административного штрафа от 500 до 1000 руб (на граждан) и от 4000 до 5000 руб (на должностных лиц)

За разглашение пользователем коммерческой тайны предусмотрена

ОТВЕТСТВЕННОСТЬ

УГОЛОВНАЯ ст. 183 п.2 УК РФ

Наказывается штрафом в размере 120 000 руб или лишением свободы сроком до трех лет



Типичные причины нарушений пользователей

- ▶ Самовольное создание и использование разделяемых сетевых ресурсов

Действие:

самовольное создание совместно используемых сетевых ресурсов (папок общего пользования) на своих компьютерах, несанкционированное удаление или изменение прав доступа к ним

Последствия:

создание дополнительных угроз вирусного проникновения и НСД, связанных с потерей данных или компрометацией конфиденциальных сведений, затруднение резервного копирования и контроля обмена данными

Контрмеры:

повышение ответственности пользователей, использование настроек ОС (отключение служб, настройка сетевых фильтров и т.п.)



Типичные причины нарушений пользователей

- ▶ Личная (непроизводственная) переписка по электронной почте

Действие:

злоупотребления при осуществлении личной переписки по электронной почте, претензии сотрудников на тайну личной переписки

Последствия:

непроизводительная трата ресурсов и рабочего времени (снижение продуктивности работы сотрудников), создание помех технологическим процессам, внутренние конфликты, подрыв репутации ГК «Росатом»

Контрмеры:

повышение ответственности сотрудников, подписание соглашений о контроле за перепиской



Типичные причины нарушений пользователей

- ▶ Пересылка конфиденциальных сведений ГК «Росатом» в открытом виде

Действие:

пересылка конфиденциальной корпоративной информации в открытом виде, отправка писем посторонним лицам по ошибочным адресам, использование дополнительных личных почтовых ящиков на внешних (сторонних) почтовых серверах и т.п.

Последствия:

утечка конфиденциальной информации
(в том числе коммерческих секретов)

Контрмеры:

повышение ответственности, применение Защищенной корпоративной почтовой системы

Пересылка конфиденциальных сведений ГК «Росатом» осуществляется установленным порядком с помощью защищенных с использованием шифровальных (криптографических) средств систем



Типичные причины нарушений пользователей

- ▶ Использование доступа в Интернет в непроизводительных целях
- ▶ Посещение хакерских или взломанных хакерами сайтов

Действие:

посещение сторонних сайтов (информационных, развлекательных, электронных магазинов или каталогов и т.п.), загрузка различных файлов, посещение хакерских или взломанных хакерами (зараженных) и других подозрительных сайтов (содержащих ловушки и вредоносные коды)

Последствия:

непроизводительные затраты ресурсов, создание помех основным технологическим процессам, вирусное заражение, загрузка троянских и других вредоносных программ, возможность обвинения во взломе данных сайтов, непреднамеренная пересылка конфиденциальной информации («фишинг»)

Контрмеры:

повышение ответственности пользователей, установка средств фильтрации трафика по адресам сайтов, безопасная настройка Web-клиентов



Приказ от 16.04.2014 №1/375-П



РОСАТОМ

п. 3.1.9 Средства вычислительной техники предоставляемые работнику для выполнения служебных обязанностей не предназначены для хранения и обработки личной информации

п. 4.2 Пользователь обязан:

- ▶ п. 4.2.1: Использовать ИРС только в целях исполнения своих должностных обязанностей;

п. 4.3 Пользователю запрещается:

- ▶ п. 4.3.9: Использовать предоставленные в пользование средства вычислительной техники и ИРС для хранения и обработки информации, не имеющей отношения к выполнению своих должностных или иных обязанностей.



ГРИНАТОМ

Типичные причины нарушений пользователей

- ▶ Нарушение правил использования средств криптографической защиты информации

Действие:

нарушение правил применения средств криптографической защиты информации

Последствия:

утрата криптографических ключей, требующая их замены в системе (выход из строя ключевого носителя). Компрометация секретных ключей, используемых для шифрования и ЭП файлов и защиты удаленного взаимодействия. Злоумышленник может получить доступ к зашифрованной конфиденциальной информации, доступ в корпоративную сеть с правами пользователя скомпрометированного ключа, а также в случае компрометации секретного ключа ЭП может подделывать подписи его владельца

Контрмеры:

обучение пользователей правилам работы со средствами криптографической защиты информации (СКЗИ), сдача зачетов по программе обучения

К самостоятельной работе к СКЗИ допускаются пользователи сдавшие зачеты по программе обучения правилам работы с СКЗИ. Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты (ОКЗ). Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего ОКЗ на основании принятых от этих лиц зачетов по программе обучения.



Требования к эксплуатации СКЗИ

- ▶ Средствами СКЗИ **НЕ ДОПУСКАЕТСЯ** обрабатывать информацию, содержащую сведения, составляющие государственную тайну;
- ▶ Ключевая информация является конфиденциальной;
- ▶ Срок действия ключа проверки ЭП – не более 15 лет после окончания срока действия соответствующего ключа ЭП (определяется при сертификации СКЗИ);
- ▶ СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах;
- ▶ Установка СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.



Требование к размещению технических средств с установленными СКЗИ

- ▶ Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию
- ▶ Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.



Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе

Требования к программному и аппаратному обеспечению

- ▶ На технических средствах, оснащенных СКЗИ должно использоваться только лицензионное программное обеспечение фирм-производителей, либо ПО, сертифицированное ФСБ. Указанное ПО не должно содержать средств разработки или отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ;
- ▶ На ПЭВМ одновременно может быть установлена только одна разрешенная ОС;
- ▶ В BIOS ПЭВМ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС;
- ▶ Средствами BIOS должна быть отключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем;
- ▶ Вход в BIOS должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС;
- ▶ Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
- ▶ Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация);
- ▶ Запрещается подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- ▶ Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.



Правила использования и хранения ключевых носителей

ЗАПРЕЩАЕТСЯ:

- ▶ оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации; при уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- ▶ вносить какие-либо изменения в программное обеспечение СКЗИ; в случае исчезновения на компьютере системы использующей средства криптографической защиты – сообщить в службу информационной безопасности и прекратить работу с любой доступной на компьютере системой до выявления причины;
- ▶ осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- ▶ разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- ▶ разглашать пароль другим лицам;
- ▶ записывать на ключевые носители постороннюю информацию;

Федеральный закон от 06.04.2011 №63 ФЗ «Об электронной подписи»

ст.10 п.1 При использовании усиленных электронных подписей участники электронного взаимодействия обязаны: обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия



При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Ключевые носители должны храниться в опечатываемых пеналах, которые в свою очередь необходимо помещать в опечатываемые сейфы. Пользователь несет персональную ответственность за хранение личных ключевых носителей.



Приказ от 09 февраля 2005 г. № 66



пп. 46 СКЗИ эксплуатируются в соответствии с правилами пользования ими...

пп. 51 Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

- ▶ обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
- ▶ собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
- ▶ ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.



Компрометация ключей

Компрометация – любая возможность (или совершившийся факт) попадание ключей посторонним (не допущенным) лицам

утрата
ключевого
носителя с
последующим
обнаружением

увольнение
сотрудников,
имевших
доступ к
ключевой
информации

временное
оставление
ключевого
носителя без
присмотра

нарушение
печатей на
сейфе с
ключевыми
носителями

нарушение
печатей
пеналов, в
которых
хранятся
ключевые
носители

случаи, когда
нельзя
достоверно
установить, что
произошло с
ключевыми
носителями

В случае утери действующего ключевого носителя с ЭП, а также обнаружения после потери – немедленно направить администратору безопасности сообщение о компрометации ключей ЭП



Типичные причины нарушений пользователей

- Нарушение правил использования средств защиты от несанкционированного доступа

Действие:

использование простых для подбора паролей, работа под чужими именами (с чужими паролями), передача или утрата атрибутов разграничения доступа к ресурсам системы (паролей, идентификационных устройств, пропусков и т.п.)

Последствия:

любой возможный ущерб от несанкционированного доступа к ресурсам системы постороннего лица с правами владельца утраченных реквизитов разграничения доступа

Контрмеры:

повышение ответственности и контроля, внедрение многофакторной аутентификации

Ошибки при использовании паролей

Пользователи очень любят записывать пароли

Пользователи придумывают пароли которые легко угадать

Пользователи обсуждают свои пароли вслух при посторонних

Пользователи часто оставляют компьютер включенным без присмотра

Приказ от 16.04.2014 №1/375-П



п. 4.3 Пользователю запрещается:
п. 4.3.8 Оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного доступа

Заблокировать компьютер:



или
Ctrl-Alt-Del + Enter



Меры предосторожности при работе с паролями

- ▶ Позаботьтесь, чтобы при вводе пароля за Вами не подглядывали (в том числе и с помощью камер видеонаблюдения);
- ▶ Когда вам оказывают техническую поддержку, всегда вводите свой пароль сами и никогда не выдавайте его;
- ▶ Не вводите свой пароль на чужих компьютерах;
- ▶ Не используйте один и тот же пароль для доступа к внутренним ресурсам ГК «Росатом» и для доступа к службам в сети Интернет;
- ▶ Периодически меняйте свой пароль. Следуйте правилам придумывания стойких и запоминающихся паролей;
- ▶ Если необходимо записать пароль, храните его в физически наиболее безопасном месте (в личном сейфе), либо используйте утвержденные ИБ программно-аппаратные средства;
- ▶ Если Вас кто-либо под каким-либо предлогом попросит сообщить Ваш пароль (социальный инжиниринг, «фишинг»), не поддавайтесь на уловку и незамедлительно доложите об этом Администратору безопасности.



Правила придумывания стойких и запоминающихся паролей



Использование
парольных фраз вместо
отдельных слов:

True_rule1



Выборочная замена букв
в осмысленном слове
специальными символами

p@ssW0rd Pa\$\$w0rd
p@\$w0rD



Добавление символов в
начале (в середине, в
конце) парольной фразы

----True__rule2----



Использование
ассоциаций (букв из
ключевых фраз)

Приказ от 16.04.2014 №1/375-П



РОСАТОМ

п.3.1.10 С целью соблюдения принципа персональной ответственности за свои действия, каждому пользователю, допущенному к работе с конкретным ИРС, используется индивидуальный уникальный идентификатор (учетная запись) и пароль, а в отдельных случаях – закрытый ключ аутентификации пользователя и его сертификат открытого ключа. Индивидуальный пароль служит для проверки подлинности (аутентификации) пользователя при доступе к ИРС и должен сохраняться им в тайне. Определенной категории работников, в случае производственной необходимости, могут быть присвоены несколько уникальных имен (учетных записей). Использование при работе несколькими пользователями одного и того же имени пользователя («группового имени») запрещено.



РОСАТОМ

Ответственность

для лиц, допустивших нарушения требований по защите конфиденциальной информации

Трудовой кодекс РФ

ст. 81 Расторжение трудового договора по инициативе работодателя

Трудовой договор может быть расторгнут работодателем в случаях:

...
б) однократного грубого нарушения работником трудовых обязанностей:

...
в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.



Уголовный кодекс РФ

- ст. 137** Нарушение неприкосновенности частной жизни;
- ст. 138** Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;
- ст. 183** Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну;
- ст. 272** Неправомерный доступ к компьютерной информации;
- ст. 273** Создание, использование и распространение вредоносных программ для ЭВМ;
- ст. 274** Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети;
- ст. 293** Халатность;
- ст. 171** Незаконное предпринимательство;



**Наказание до 7 лет лишения свободы
штраф до 300 000 руб.**

Кодекс РФ об административных правонарушениях

ст. 13.11 Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

ст. 13.12 Нарушение правил защиты информации;

ст. 13.14 Разглашение информации с ограниченным доступом;



**Штраф до 30 000 руб. с конфискацией,
приостановление деятельности
на срок до 90 суток**



**Самая большая ошибка - игнорирование установленных ограничений
и правил политики безопасности при работе системы**



**Будьте внимательны и осторожны!
Помните об угрозах ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ!**



ГРИНАТОМ