Как повысить эффективность использования технических средств ИБ.

...и причём тут дорожная полиция?

ОБОМНЕ

- Туговиков Виктор Борисович,
- Сибирский федеральный университет,

  Кафедра прикладной математики и компьютерной безопасности,

  Научно-учебная лаборатория Информационной безопасности,

  доцент, к.ф.м-н.

  Эксперт в области построения систем управления информационной безопасностью. В отрасли с 1997 года.

  VTugovikov@sfu-kras.ru

  +79080261392

О чём речь:

Что такое защита информации, информационная безопасность – в настоящее время в определённой мере понимают даже не специалисты.

Тем не менее, а может и в связи с этим, у руководителей организаций порой складывается мнение, что нужно выполнить «бумажную безопасность», приобрести требуемые по закону средства защиты информации, грамотно их настроить, раздать работникам памятки на тему «информационная безопасность» и проблема решена.

О чём речь:

Но случается, что даже после установки и настройки технических средств, раздачи памяток, происходит инцидент и организация теряет деньги, теряет клиентов, конкурентные преимущества, страдает репутация и пр..

Возникают вопросы:
Кто виноват и что делать?
Приобретать более дорогие средства защиты?
Докупать модули к уже закупленным системам?

Инсайдеры - корень зла в инфобезе?

Приобретать более дорогие средства защиты?
Докупать модули к уже закупленным системам?

Что делать?

Вариант 1: приобретение и установка СЗИ, которые могут блокировать нарушения ИБ «на лету».

Вариант 2: запретить (частично) использование каналов информационного обмена, передачи информации, которые могут быть использованы для нарушения ИБ.

Вариант 3: привлечь весь персонал к вопросам обеспечения ИБ.

КИБЕРДРУЖИНА

Как привлечь персонал к вопросам обеспечения ИБ:

1. Повышение IT – грамотности.
2. Повышение ИБ – грамотности.
3. Возложение ответственности за выполнение мер ИБ на пользователей.
4. Возложение ответственности за выполнение мер ИБ на руководителей.
5. Контроль выполнения мер ИБ.

КИБЕРДРУЖИНА

Контроль выполнения мер ИБ:

Подход: «дорожная полиция»

Контроль выполнения мер ИБ:

Контроль выполнения мер ИБ:

Приложение

к Приказу № _____ от «___» _____ 2022 г.

Инструкция по обеспечению информационной безопасности при использовании ресурсов и сервисов компьютерной сети ОАО «Химфармтаблетка»

Сотрудник ОАО «Химфармтаблетка» (далее – Сотрудник) несет персональную ответственность за соблюдение требований настоящей Инструкции. Руководитель структурного подразделения несет ответственность за своевременное и надлежащее ознакомление подчиненных ему сотрудников с настоящей Инструкцией и осуществление контроля соблюдения ее требований.

Контроль выполнения мер

1. Используемые термины:

Сотрудник – физическое лицо, работающее по трудовому договору или договору граждан правового характера в ОАО «Химфармтаблетка».

Режим коммерческой тайны – это правовые, организационные, технические и и принимаемые обладателем информации, составляющей Коммерческую тайну, мер охране ее конфиденциальности.

Защищенный канал передачи данных – канал передачи данных, в котором информа преобразована таким образом, чтобы отсутствовала возможность ознакомления тр лиц с передаваемыми данными.

КС – компьютерная сеть ОАО «Химфармтаблетка»

Ресурсы КС – различные информационные ресурсы и сервисы (компьютеры, сетевые ди электронная почта, WEB-портал, и т.п.), предоставляемые КС сотрудникам выполнении служебных обязанностей.

Служебный компьютер –компьютер переданный сотруднику во временное пользование выполнения его должностных обязанностей.

Переносной компьютер – компьютер, предназначенный для перемещения и оснащен аккумулятором (ноутбук, смартфон, КПК, iPad и пр.).

Доступ к информации – возможность санкционированного ознакомления с информацией копирования, модификации или уничтожения.

Посторонние лица – физические лица, которые не являются сотрудниками О «Химфармтаблетка» или не имеют допуска для работы с коммерческой тайной, дру информацией конфиденциального характера.

СИБ – специалист (служба) информационной безопасности, уполномоченный приним решения по вопросам информационной безопасности и режима коммерческой тай

Беспроводные устройства – технические устройства, позволяющие передавать и принима компьютерную информацию без использования проводов.

Мобильные носители информации – диски и карты памяти цифровых устройств, фл карты, дискеты, компакт-диски, оптические диски, магнитные ленты, USB-устройс беспроводные устройства накопления информации и другие физические устройств которые возможна запись и хранение компьютерной информации.

Несанкционированный доступ – доступ к информации, предпринимаемый в об установленных правил, без письменного согласования или разрешения владел информации (информационного ресурса) или его законного представителя.

Реквизиты доступа – имя пользователя (логин), и пароль.

Компрометация пароля – возникновение условий для получения личного пароля Сотруд другими лицами, установление факта передачи пароля Сотрудником другому лицу факта работы под именем Сотрудника в период его фактического отсутствия.

Контроль выполнения мер

2. **Сотрудник обязан:**

2.1. Знать и соблюдать требования информационной безопасности, режима коммерческой тайны в соответствии с действующими локальными нормативными актами.

2.2. Использовать предоставленные ему служебные информационно-вычислительные ресурсы и сервисы только в служебных целях в соответствии с должностными обязанностями и служебными потребностями.

2.3. Применять все необходимые меры по недопущению посторонних лиц к ресурсам КС.

2.4. Обеспечивать блокирование доступа к работающему компьютеру во время отсутствия Сотрудника на рабочем месте.

2.5. При обнаружении или подозрении на несанкционированный доступ к служебному компьютеру или какому-либо ресурсу КС незамедлительно доложить об этом своему руководителю и уведомить о случившемся СИБ.

2.6. При получении писем электронной почты, прочих сообщений от неизвестных, подозрительных источников незамедлительно доложить об этом своему руководителю и уведомить о случившемся СИБ.

2.7. При проявлении на компьютере подозрительной активности незамедлительно обратиться к IT-специалистам, уведомить о случившемся СИБ.

2.8. **В рамках выполнения правил парольной защиты:**

2.8.1. Хранить в тайне имя пользователя и пароль, используемые для доступа к ресурсам КС.

2.8.2. Незамедлительно сменить пароль в случае компрометации пароля и доложить о случившемся своему руководителю, уведомить СИБ.

2.8.3. Передавать кому-либо свои реквизиты доступа к КС или ее ресурсам только по письменному распоряжению руководителя, согласованному с СИБ. В распоряжении руководителя должно быть указано обоснование передачи пароля, конкретный срок, на который передается пароль.

2.8.4. По окончании использования реквизитов доступа другим работником, Сотрудник обязан сменить все пароли, которые были предоставлены другому лицу.

2.9. **При работе с конфиденциальной информацией.**

2.9.1. Применять все необходимые меры по сохранению конфиденциальности информации, используемой в своей служебной деятельности.

2.9.2. Хранить файлы и папки, содержащие конфиденциальную информацию, только в специально выделенных ресурсах КС, в том числе в специально выделенных папках или файл-дисках на локальном компьютере Сотрудника.

2.9.3. При использовании мобильных носителей для конфиденциальной и служебной информации применять только выделенные для этих категорий информации носители.

2.9.4. Осуществлять контроль за электронными документами, файлами с конфиденциальной информацией, которые распечатываются на сетевом принтере, бумажными носителями, которые сканируются на сканере, копируются на копировальном аппарате, с целью недопущения несанкционированного доступа к обрабатываемой информации других лиц.

2.9.5. При уничтожении распечаток осуществлять контроль за полным уничтожением распечатанной конфиденциальной информации в уничтожителе бумаги (документов).

2.9.6. Осуществлять защиту конфиденциальной информации при её отправке с использованием электронной почты. Методы защиты должны быть согласованы с СИБ.

2.9.7. Использовать только защищенные, согласованные с СИБ каналы передачи данных при обмене конфиденциальной информацией с контрагентами, другими внешними организациями.

2.9.8. Использовать согласованное с СИБ программное обеспечение для защиты информации при копировании конфиденциальной информации на мобильные носители или переносной компьютер.

Контроль выполнения мер

3. Сотруднику запрещено:

3.1. Осуществлять доступ или попытки доступа к информационно-вычислительным ресурсам и сервисам в нарушение установленных правил предоставления доступа, путем подбора, хищения пароля, запуска программ «взлома» парольной защиты и т.п.

3.2. Использовать какое-либо программное обеспечение для сканирования, поиска уязвимостей и осуществления каких-либо подобных действий в КС, отдельных ее узлах, в отношении отдельных сетевых устройств.

3.3. Выполнять самостоятельно действия, связанные с:

а) разборкой (вскрытием корпуса), внесением изменений в конфигурацию служебного компьютера и/или периферийного оборудования;

б) подключением/отключением к сетевым разъемам и портам КС (кроме сотрудников, работающих с переносными компьютерами, а также за исключением случаев решения проблем с помощью сотрудников технической поддержки);

в) изменением параметров программного обеспечения, операционной системы, периферийного оборудования (за исключением Сотрудников, чьи должностные обязанности предусматривают данные процедуры).

3.4. Подключать мобильные носители информации, беспроводные устройства без письменного согласования с СИБ.

3.5. Использовать мобильные носители информации для хранения, записи и воспроизведения информации, не связанной с выполнением своих должностных обязанностей.

3.6. Использовать в личных, непроизводственных целях доступ к сети Интернет, электронную почту, папки и файлы, расположенные на сетевых серверах и служебных компьютерах.

3.7. При подключении к Интернет использовать анонимайзеры и другие ресурсы и способы маскировки своих действий.

3.8. Использовать для отправки сообщений, сайты Интернет, другие ресурсы, не входящие в состав КС, без согласования с СИБ.

3.9. Осуществлять подписку на личный корпоративный адрес электронной почты различных почтовых рассылок и уведомлений, не связанных со служебной необходимостью.

3.10. Без согласования с СИБ копировать данные, документы и иную служебную информацию на ресурсы, не относящиеся к ресурсам КС (ресурсы Интернет, сторонние серверы FTP, и т.п).

3.11. Хранить, записывать, копировать на служебный компьютер любую информацию, не связанную с выполнением должностных обязанностей (аудио-, видеофайлы, экранные заставки и другие компьютерные данные).

3.12. При наличии прав локального администратора на рабочем компьютере без письменного согласования с СИБ:

а) Инсталлировать либо удалять программное обеспечение.

б) изменять права локальных пользователей и групп;

в) открывать для кого-либо сетевой доступ к локальным ресурсам служебного компьютера;

г) создавать новых локальных пользователей и группы;

д) организовывать доступ в сеть Интернет через модемы;

е) подключать к рабочему компьютеру какое-либо оборудование (мобильные носители информации, фотоаппараты, мобильные телефоны, плееры, модемы и т.п.);

ж) устанавливать, использовать и хранить (включая установочные копии) программное обеспечение:

- приобретенное с нарушением законодательства РФ;
- не входящее в перечень действующего на предприятии стандарта программного обеспечения;
- не связанное с выполнением должностных обязанностей.

3.13. **В рамках выполнения правил парольной защиты:**

3.13.1. Хранить свои и вверенные для временного использования реквизиты доступа к КС и отдельным программам и защищенным ресурсам в местах, не предназначенных для обработки конфиденциальной информации: в общедоступных информационных ресурсах, на

Контроль выполнения мер ИБ:

Я согласен (согласна), что мои действия, производимые с использованием сервисов и ресурсов КС будут контролироваться службой безопасности и СИБ ОАО «Химфармтаблетка».

Несоблюдение данной инструкции расценивается как нарушение установленных правил информационной безопасности, создание рисков нанесения ущерба ОАО «Химфармтаблетка» (целенаправленно либо по халатности) и влечет за собой привлечение к дисциплинарной, административной, уголовной ответственности в соответствии с действующим законодательством.

С инструкцией ознакомлен (-на):

_____

Фамилия, Имя, Отчество полностью

_____

_____

должность

_____

_____

подразделение

_____

Дата:	_____	**Подпись**:	_____

Агитпроп от Касперского

Правила информационной безопасности для персонала.
В зоне доступа к ЗО КИИ ЗАПРЕЩАЕТСЯ:

1

Передавать конфиденциальные файлы через внешние облачные сервисы

2

Проверять личную почту через рабочие станции промышленной сети

Правила информационной безопасности для персонала.
В зоне доступа к ЗО КИИ ЗАПРЕЩАЕТСЯ:

3

Скачивать файлы из внешних источников в промышленную сеть

4

Использовать социальные сети и сервисы на рабочем месте

Правила информационной безопасности для персонала.
В зоне доступа к ЗО КИИ ЗАПРЕЩАЕТСЯ:

5

Развертывать собственные Wi-Fi сети на территории промышленных объектов

6

Загружать постороннее ПО на рабочие станции промышленной сети

Правила информационной безопасности для персонала.
В зоне доступа к ЗО КИИ ЗАПРЕЩАЕТСЯ:

7

Использовать камеры в личных мобильных устройствах

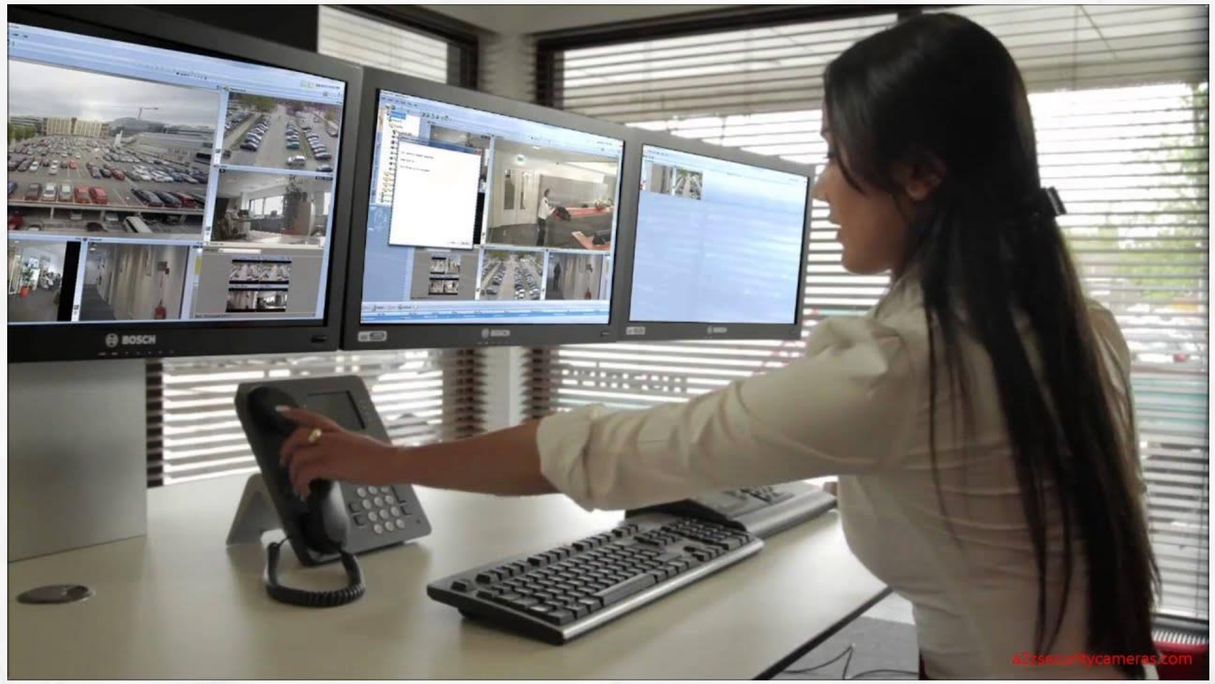
8

Использовать посторонние USB-накопители

Правила информационной безопасности для персонала.
В зоне доступа к ЗО КИИ ЗАПРЕЩАЕТСЯ:

Взаимодействие ИБ с IT:

Для сетевых администраторов, администраторов систем, нужны отдельные инструкции, ориентированные на правила выполнения ИБ привилегированными пользователями.



Взаимодействие ИБ с IT:

Приложение

к Приказу № _____ от «___» _____ 20XX г.

Инструкция администратору компьютерной сети ООО «Химфармтаблетка» по выполнению мер информационной безопасности.

Администратор компьютерной сети (КС) несет персональную ответственность за выполнение правил и требований по обеспечению информационной безопасности ООО «Химфармтаблетка» (далее по тексту **ОРГАНИЗАЦИЯ**).

Допуск работников к функциям администрирования элементами КС разрешается по согласованию со службой безопасности ОРГАНИЗАЦИИ, после изучения ими требований данной инструкции, других нормативных и организационно - распорядительных документов по информационной безопасности, подписания соответствующих обязательств о неразглашении конфиденциальной информации.

Самовольное нарушение администраторами КС правил разграничения доступа является нарушением Обязательств о неразглашении конфиденциальной информации ОРГАНИЗАЦИИ и влечет за собой привлечение к материальной, уголовной и другой ответственности, предусмотренной законодательством РФ.

Взаимодействие ИБ с IT:

5. Администратор КС несет личную ответственность:

5.1. За разглашение либо использование без согласования с СИБ известных ему паролей доступа к информационным ресурсам, а также за разглашение любой конфиденциальной информации ОРГАНИЗАЦИИ, ставшей ему известной в ходе выполнения работ или при других обстоятельствах.

5.2. За установку и эксплуатацию на СВТ и ресурсах КС ОРГАНИЗАЦИИ (специально или по халатности) программного обеспечения, не содержащегося в списке рекомендованного к использованию на предприятии, содержащего вредоносные программы или программные закладки.

Я согласен (согласна), что мои действия, производимые с использованием сервисов и ресурсов КС будут контролироваться службой безопасности и СИБ ОАО «Химфармтаблетка».

Несоблюдение данной инструкции расценивается как нарушение установленных правил информационной безопасности, создание рисков нанесения ущерба ОАО «Химфармтаблетка» (целенаправленно либо по халатности) и влечет за собой привлечение к дисциплинарной, административной, уголовной ответственности в соответствии с действующим законодательством.

С инструкцией ознакомлен (-на):

_____

Фамилия, Имя, Отчество полностью

В заключение:

Готов ответить на ваши вопросы

E-mail: tuemok@mail.ru
+79080261392