Положение

о контроле защищенности конфиденциальной информации

Общие положения

1) Настоящее положение определяет порядок выявления, анализа и устранения уязвимостей, недостатков программного обеспечения, аппаратных средств, организационно-технических недостатков и порядок действий ответственных лиц ОГБУЗ ГБ г. Костромы (далее – Организация) при контроле защищенности конфиденциальной информации, обрабатываемой в информационных системах (Далее -ИС) Организации.
2) В данном положении описаны правила и процедуры обеспечения целостности и доступности информации в ИС Организации.
3) Действие настоящего положения распространяется на всех сотрудников Организации и третью сторону в части их касающейся.

Выявление анализ и устранение уязвимостей

1) Уязвимость – это недостаток ИС или системы защиты, который может привести к реализации угрозы безопасности информации.
2) Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы.
3) Периодичность плановых процедур выявления, анализа и устранения уязвимостей ИС составляет 1 год. Внеплановые процедуры выявления, анализа и устранения уязвимостей ИС проводят по распоряжению ответственного за организацию информационной безопасности в случае необходимости. Необходимость внеплановой процедуры выявления и устранения уязвимостей определяет администратор безопасности на основе фактов, которые свидетельствуют о возможной угрозе. В обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИС.
4) В ИС должно осуществляться выявление и устранение следующих типов уязвимостей:

- Ошибки кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
- Недостатки аппаратных средств ИС, в том числе аппаратных средств защиты информации;
- Организационно-технические недостатки.

5) В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.
6) Системный администратор организует получение из доверенных источников и установку обновлений базы признаков уязвимостей.
7) Мероприятия по выявлению, анализу и устранению уязвимостей организует администратор безопасности. Непосредственными исполнителями мероприятий по выявлению уязвимостей ИС является комиссия по информационной безопасности Организации, в которую в обязательном порядке входит Администратор безопасности.
8) В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования

информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

9) Результат проведенных мероприятий по выявлению, анализу и устранению уязвимостей закрепляется в акте проверки (**приложение №1)**

Уязвимости программного обеспечения

1) Анализ программного обеспечения включает:

- Проверка наличия и сроков действия лицензий на установленное программное обеспечение ИС;
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации:
  - Контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
  - Проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;
  - Контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;
  - Восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.
- Проверка наличия последних обновлений используемого программного обеспечения ИС:
  - Проверка обновлений вирусных баз;
  - Проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.
  - Проверка обновлений баз решающих правил для средств обнаружения вторжений (*при использовании средств обнаружения вторжений*);
- Проверка обновлений баз признаков уязвимостей.

2) Устранение обнаруженных недостатков на основании своих полномочий осуществляют администратор безопасности и привлеченные им для этого лица.

Уязвимости аппаратных и технических средств

1) К недостаткам аппаратных и технических средств, используемых в ИС, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

2) При выявлении недостатков аппаратных и технических средств проверяют:

- Техническое состояние аппаратных средств;
- Наличие сертификатов соответствия на примененные в ИС и ее системе защиты информации аппаратные средства;
- Наличие у поставщиков обновленных версий аппаратных средств, примененных в ИС и системе защиты информации;
- Перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств;
- Конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

3) Обнаруженные в ходе проверки отклонения от конфигурации ИС устраняет администратор безопасности и системные администраторы, каждый в своей части.

4) При обнаружении аппаратных средств с низкой надежностью, частыми выходами из строя системный администратор принимает меры по ремонту или замене этих аппаратных средств.

Организационно – технические уязвимости

1) Проверка организационно-технической составляющей включат:

- Проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите конфиденциальной информации, обрабатываемых в ИС;
- Проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД);
- Проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям**;**
- Проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям**;**
- Проверка соответствия правилам обработки и защиты ПДн;
- Проверка соответствия выполнения правил разграничения доступа к ресурсам ИС принятым требованиям;
- Проверка соответствия полномочий пользователей принятым требованиям;
- Проверка состояния физической защиты ИС (средства охраны и физического доступа в контролируемых зонах ИС);
- Проверка знания и соблюдения пользователями ИС основных нормативно-правовых актов в области защиты конфиденциальной информации и требований ОРД;
- Проверка состава технических средств, программного обеспечения и средств защиты информации (инвентаризация). В информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.

2) В ИС должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей;

3) В проверке обязательно непосредственно участвует администратор безопасности.

Обеспечение целостности ИС и обрабатываемой информации

1) В Организации в обязательном порядке должна быть организована система обеспечения целостности ИС и обрабатываемой ей информации.

2) Обеспечение целостности осуществляется на постоянной основе администратором безопасности и системными администраторами.

3) Обеспечение целостности должно включать:

- Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, который предусматривает:

o Контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы;

o Контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;

o Контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;

- Тестирование функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств;
- Контроль целостности средств защиты информации по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;
- Исключение возможности использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды.

- Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама), которое предусматривает:

- Реализацию на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам;
- Фильтрацию по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;
- Фильтрацию на основе информации об отправителе электронного сообщения (в том числе с использованием "черных" списков (запрещенные отправители) и (или) "белых" списков (разрешенные отправители);
- Обновление базы "черных" ("белых") списков и контроль целостности базы "черных" ("белых") списков.

Обеспечение доступности информации

1) В Организации в обязательном порядке должна быть организована система обеспечения доступности информации.
2) Обеспечение доступности осуществляется на постоянной основе администратором безопасности и системными администраторами.
3) Обеспечение доступности должно включать:

- Резервное копирование информации, а именно:

- Резервное копирование информации на резервные машинные носители информации;
- Разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;
- Регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;
- Принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность;
- Проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий;
- Хранение (размещение) резервных копий информации на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.

- Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала, а именно:
  - Определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации;
  - Восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;
  - Регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.
- Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций, которое предусматривает:
  - Планы по действиям персонала при возникновении нештатных ситуаций;
  - Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;
  - Возможность восстановления и проверки работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;
  - Возможность возврата информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, позволяющих решать задачи по обработке информации;
  - Систему компенсирующих мер защиты информации, когда восстановление работоспособности системы защиты информации невозможно.
- Контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривающий:
  - Контроль выполнения провайдером требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения);
  - Мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей);
  - Мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) услуг по передаче информации.

Заключительные положения

1) Сотрудники Организации должны быть предупреждены об ответственности за действия, нарушающие требования настоящего положения.
2) Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим положением, в пределах, определенных действующим законодательством Российской Федерации и локальными актами организации.

Приложение №1

Акт проведенной проверки информационной безопасности

В ходе проверки объекта защиты информации _____

_____

(Указать наименование объекта)

Расположенного по адресу : _____

_____

(Указать адрес объекта)

Было установлено:

Объект: Имеет уязвимости | Не имеет уязвимостей

(Нужное подчеркнуть)

Уязвимости программного обеспечения

_____

_____

_____

_____

_____

_____

_____

Уязвимости аппаратных средств

_____

_____

_____

_____

_____

_____

_____

Организационно – технические уязвимости

Предпринятые действия для устранения уязвимостей

Дополнительные пояснения по процессу проверки

Администратор безопасности) _____

Дата:_____ МП