Приложение 5
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

ПОЛИТИКА
сетевой безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Политика сетевой безопасности (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация) регулирует вопросы обеспечения сетевой безопасности локально-вычислительной сети образовательной организации как части комплекса мер по обеспечению безопасности информации в образовательной организации.

1.2. Настоящая Политика разработана в соответствии с:

1.2.1 приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.2 приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.2.3 методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

1.3. Настоящая Политика определяет требования сетевой безопасности, технологии и механизмы обеспечения безопасности сетевой инфраструктуры, а также принципы управления сетевой безопасностью.

2. Общие требования по обеспечению сетевой безопасности

2.1. Локально-вычислительная сеть (далее – ЛВС) является составной частью информационных систем образовательной организации, обеспечивающая его функционирование.

2.2. ЛВС подлежит защите от воздействий (как внутренних, так и внешних), которые могут привести к:

2.2.1 нарушению непрерывности функционирования информационных процессов;

2.2.2 нарушению конфиденциальности защищаемой информации;

2.2.3 целостности защищаемой информации и правил разграничения доступа к информационным ресурсам.

2.2.4 нарушению доступности защищаемой информации и сервисов информационных систем.

2.3. Средства, используемые в составе ЛВС для обеспечения необходимого уровня безопасности информации, должны обеспечивать:

2.3.1 доступность, целостность и конфиденциальность информационных ресурсов;

2.3.2 защиту каналов передачи данных и управления, доступность данных каналов;

2.3.3 защиту сетевого трафика от перехвата;

2.3.4 защищенный удаленный доступ в информационную систему;

2.3.5 простоту используемых технологий защиты информации и их эксплуатации;

2.3.6 прозрачность используемых средств и механизмов защиты для пользователей.

2.4. С целью обеспечения выполнения указанных требований в составе ЛВС должны применяться следующие технологии сетевой безопасности:

2.4.1 межсетевое экранирование;

2.4.2 обнаружение и предотвращение вторжений;

2.4.3 криптографическая защита информации.

2.5. С целью минимизации возможных точек доступа к сетям связи общего пользования (в том числе сети интернет) использование технологий беспроводной передачи данных в образовательной организации запрещено.

2.6. Для регистрации сетевых узлов (автоматизированных рабочих мест, серверов и активного сетевого оборудования) в сети используются физические адреса (MAC-адреса) и IP-адреса. Для каждого сетевого узла задается IP-адрес маршрутизатора (адрес шлюза по умолчанию), через который он может связываться с компьютерами в других локальных сетях и сети Интернет. Присваивание этих параметров производится автоматически функционалом DHCP-сервера.

2.7. Доступ к средствам (устройствам) сетевой безопасности предоставляется работникам, наделенным соответствующими полномочиями.

3. Межсетевое экранирование

3.1. Средствами межсетевого экранирования должен реализовываться следующий функционал:

3.1.1 идентификация сетевых устройств по IP-адресам и (или) MAC-адресам;

3.1.2 аутентификация сетевых устройств, по одному из протоколов: Remote Authentication Dial-In User Service (RADIUS); Terminal Access Controller

Access Control Systems (TACACS); Lightweight Directory Access Protocol (LDAP); Kerberos;

3.1.3 фильтрация информационных потоков по протоколам (например, TCP, UDP, IP), портам и адресам назначения, а также определение маршрутов передачи информации (требования к фильтрации устанавливаются в соответствии с заявками пользователей на доступ к информационным ресурсам (системам) в порядке, установленном Политикой использования информационных активов государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий», а также потребностями администраторов, обусловленными необходимостью администрирования информационных ресурсов (систем) и средств обработки информации);

3.1.4 завершение сетевых соединений (например, откреплением пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного Администратором временного интервала неактивности сетевого соединения);

3.2. С целью выполнения указанных требований могут применяться:

3.2.1 программные и программно-аппаратные средства межсетевого экранирования уровня периметра сети – на внешней границе информационной системы;

3.2.2 программные средства межсетевого экранирования уровня хоста – на внутренних узлах сегментов информационных систем (автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем);

3.2.3 иное активное сетевое оборудование (коммутаторы, маршрутизаторы и прочее), реализующие необходимый функционал.

3.3. Используемые средства межсетевого экранирования должны иметь соответствующие действующие сертификаты соответствия, выданные ФСТЭК России.

3.4. Средства межсетевого экранирования могут интегрироваться со средствами антивирусной защиты информации с целью обеспечения антивирусной защиты информации периметра ЛВС.

4. Обнаружение и предотвращение вторжений

4.1. Система обнаружения и предотвращения вторжений (далее - СОВ) позволяет распознавать вредоносную активность внутри сети. СОВ должны иметь в своем составе следующие компоненты:

4.1.1 регистрации событий безопасности (датчики);

4.1.2 анализа событий безопасности и распознавания компьютерных атак (анализаторы);

4.1.3 базу решающих правил (базу сигнатур), содержащую информацию о характерных признаках компьютерных атак.

4.2. Средствами обнаружения вторжений должен реализовываться следующий функционал:

4.2.1 отслеживание атак в режиме реального времени;

4.2.2 использование сигнатурных и эвристических методов для анализа сетевого трафика;

4.2.3 создавать профили (наборы сигнатур, релевантных для защиты определенных сервисов);

4.2.4 задавать правила, определяющие действия для выбранного типа трафика (IP, ICMP, TCP, UDP);

4.2.5 протоколирование нештатных ситуаций, а также попыток проведения вторжений и предотвращение угроз в журнале регистраций событий, а также предоставление отчетов;

4.2.6 защита от атак на сетевые протоколы на различных уровнях модели OSI;

4.2.7 возможность анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени;

4.2.8 централизованное управление (администрирование) компонентами средств, установленными в различных сегментах информационных систем;

4.2.9 обновление (из доверенных источников) базы решающих правил;

4.2.10 контроль целостности обновлений базы решающих правил;

4.2.11 уведомление о необходимости обновления и непосредственном обновлении базы решающих правил.

4.3. Средства предотвращения вторжений должны иметь в своем составе следующие компоненты:

4.3.1 блокирование атак в режиме реального времени;

4.3.2 обрыв соединения и оповещение администратора безопасности;

4.3.3 протоколирование нештатных ситуаций в журнале регистраций событий и предоставление отчетов.

4.4. С целью выполнения указанных требований могут применяться:

4.4.1 программные и программно-аппаратные средства обнаружения вторжений уровня периметра сети – на внешней границе информационной системы;

4.4.2 программные средства обнаружения вторжений уровня хоста – на внутренних узлах сегментов информационных систем.

4.5. Используемые средства обнаружения вторжений должны иметь соответствующие действующие сертификаты соответствия, выданные ФСТЭК России.

5. Криптографическая защита информации

5.1. Средства криптографической защиты информации, передаваемой по каналам связи, должны применяться в случае, если:

5.1.1 передача защищаемой информации, в том числе персональных данных, осуществляется по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче защищаемой информации по информационно-телекоммуникационным сетям общего пользования; удаленном доступе к информационным ресурсам (системам) и средствам обработки информации, в том числе для администрирования).

5.1.2 хранение защищаемой информации осуществляется на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

5.2. Используемые средства криптографической защиты информации, передаваемой по каналам связи, должны иметь соответствующие действующие сертификаты соответствия, выданные ФСБ России.

5.3. С целью выполнения указанных требований могут применяться:

5.3.1 программно-аппаратные средства криптографической защиты информации, передаваемой по каналам связи (криптографические шлюзы) – на внешней границе информационной системы;

5.3.2 программные средства и (или) программно-аппаратные средств криптографической защиты информации (в том числе средства электронной подписи) – на внутренних узлах сегментов информационных систем (автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем).

5.4. Эксплуатация средств криптографической защиты информации, должна осуществляться в соответствии с Политикой использования средств криптографической защиты информации государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

6. Ответственность за исполнение положений настоящей Политики

6.1. Администрирование локально-вычислительной сети включает в себя реализацию следующих основных функций:

6.1.1 планирование, создание и сопровождение кабельной системы ЛВС образовательной организации;

6.1.2 организацию и сопровождение системы локальных сетей (VLAN), коммутаторов уровня доступа, магистральных коммутаторов и маршрутизаторов ЛВС образовательной организации;

6.1.3 составление и поддержку адресного плана образовательной организации;

6.1.4 организацию и сопровождение внешних каналов связи, внешней маршрутизации ЛВС Техникума с сетями Региональной мультисервисной сети органов государственной власти Краснодарского края, сетью Интернет;

6.1.5 взаимодействие с операторами связи;

6.1.6 организацию и поддержку доменной службы имен;

6.1.7 организацию и поддержку домена службы каталогов (MS Active Directory) Техникума, регистрацию объектов доменов и сопровождение их учетных записей;

6.1.8 организацию и поддержку сетевых информационных ресурсов образовательной организации в форме файловых серверов, серверов баз данных;

6.1.9 разработку и реализацию мероприятий по защите ресурсов ЛВС от несанкционированного доступа;

6.1.10 обеспечение резервного копирования и восстановления общих информационных ресурсов Техникума и информационных ресурсов структурных подразделений Техникума (по их запросам).

6.2. Администратор информационных систем несет ответственность за:

6.2.1 знание структуры локально-вычислительной сети;

6.2.2 ведение учета назначенных сетевым узлам IP-адресов;

6.2.3 настройку параметров активного сетевого оборудования в соответствии с положениями настоящей Политики;

6.2.4 настройку параметров фильтрации и маршрутизации информационных потоков в соответствии с установленными правилами;

6.2.5обеспечение резервирования критически важного активного сетевого оборудования и принятие мер по восстановлению работоспособности данного оборудования;

6.2.6 незамедлительное информирование о произошедших инцидентах, связанных с нарушением информационной безопасности (или при возникновении подозрения о возможности появления инцидента, связанного с нарушением информационной безопасности) администратора информационной безопасности.

6.3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в ЛВС и за ее пределами. В случае если с данного компьютера производился несанкционированный доступ к информации на других компьютерах и в случаях других серьезных нарушений правил пользования сетью, по решению Администратора информационной безопасности, АРМ пользователя отключается от сети, учетная запись пользователя блокируется.

6.4. Лица, виновные в нарушении положений настоящей Политики, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой и административной ответственности.