Приложение 7
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

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

1. Общие положения

1.1. Политика управления событиями безопасности информации (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация) устанавливает единый системный подход к процессу управления событиями (их регистрация, учет, сбор, хранение и обработка) 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».

1.3. Управление событиями безопасности информации осуществляется с целью своевременного выявления фактов, оказывающих негативное воздействие на информационные системы образовательной организации (выявления инцидентов информационной безопасности).

1.4. Под событием безопасности информации понимается любое проявление состояния информационной системы и системы ее защиты, указывающие на возможность:

1.4.1 нарушение конфиденциальности, целостности или доступности информации, обрабатываемой в информационной системе;

1.4.2 нарушение доступности компонентов информационной системы (АРМ, серверов, активного сетевого оборудования);

1.4.3 нарушение штатного функционирования компонентов информационных систем и средств защиты информации;

1.4.4 нарушения процедур, установленных организационно-распорядительными документами по защите информации.

1.5. Под инцидентом информационной безопасности понимается одно или серия событий безопасности информации, связанных с нарушением, установленных в образовательной организации Политик безопасности информации.

2. Регистрация, учет, сбор и хранение событий безопасности информации

2.1. Перечень событий безопасности информации, подлежащих регистрации в информационных системах образовательной организации, приведен в приложении 1 к настоящей Политике.

2.2. Перечень событий безопасности, подлежащих регистрации, должен пересматриваться, в том числе по результатам контроля (мониторинга) обеспечения уровня защищенности информации, содержащейся в информационных системах, но не реже чем 1 раз в год.

2.3. При регистрации событий безопасности информации регистрации подлежат следующие характеристики событий безопасности информации:

2.3.1 тип события безопасности информации;

2.3.2 дата и время события безопасности информации;

2.3.3 идентификационная информация источника события безопасности информации;

2.3.4 результат события безопасности информации (успешно или неуспешно);

2.3.5 субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности информации.

2.4. Источниками событий безопасности информации являются:

2.4.1 средства регистрации событий системного и прикладного программного обеспечения;

2.4.2 средства регистрации событий активного сетевого оборудования;

2.4.3 средства системы обеспечения информационной безопасности образовательной организации;

2.4.4 средства системы пожарно-охранной сигнализации и системы контроля и управления доступом;

2.4.5 работники образовательной организации;

2.4.6 работники других организаций, имеющих доступ к информационным системам образовательной организации.

2.5. Должен обеспечиваться непрерывный сбор событий безопасности информации, генерируемых компонентами информационных систем (АРМ, серверами, активным сетевым оборудованием) и средствами защиты информации.

2.6. Регистрация, учет и хранение событий безопасности информации должны обеспечиваться ответственными лицами, срок хранения событий безопасности информации должен составлять не менее 12 месяцев.

2.7. Сведения о событиях безопасности информации подлежат защите от неправомерного доступа, уничтожения или модификации. Доступ к данным сведениям должен быть ограничен, кроме уполномоченных на это лиц.

3. Мониторинг и анализ событий безопасности информации

3.1. Мониторинг и анализ событий безопасности информации осуществляется с целью выявления инцидентов информационной безопасности.

3.2. Мониторинг событий информационной безопасности может осуществляться как с использованием средств автоматизации (средств, относящихся к средствам сбора и корреляции событий безопасности информации – SIEM), так и без использования таковых.

3.3. Мониторинг и анализ событий безопасности информации осуществляется:

3.3.1 в части средств системы обеспечения информационной безопасности образовательной организации – Администратором информационной безопасности;

3.3.2 в части средств обеспечения функционирования информационных систем (системного и прикладного программного обеспечения, активного сетевого оборудования) – Администратором информационных систем. В результате анализа событий безопасности информации он должен информировать Администратора информационной безопасности о событиях, имеющих признаки инцидентов, а также непосредственно об инцидентах информационной безопасности.

3.4. Периодичность мониторинга и анализа событий безопасности информации зависит от степени критичности информационного ресурса (системы) или средства обработки информации и составляет:

3.4.1 для информационных ресурсов (систем) или средств обработки информации, имеющих высокую критичность, – ежедневно;

3.4.2 для информационных ресурсов (систем) или средств обработки информации, имеющих среднюю критичность, – не реже одного раза в неделю;

3.4.3 для информационных ресурсов (систем) или средств обработки информации, имеющих низкую критичность, – не реже одного раза в месяц.

3.5. К инцидентам информационной безопасности относятся следующие категории негативных событий (группы событий) безопасности информации:

3.5.1 разглашение защищаемой информации работниками, имеющими право доступа к ней, а именно:

3.5.1.1 передача защищаемой информации третьим лицам, не имеющим права доступа к ней;

3.5.1.2 передача защищаемой информации по открытым каналам связи;

3.5.1.3 обработка защищаемой информации на незащищенных технических средствах;

3.5.1.4 публикация защищаемой информации в СМИ;

3.5.1.5 копирование защищаемой информации на неучтенные съемные носители информации;

3.5.1.6 утрата съемных и (или) бумажных носителей информации или передача их лицам, не имеющим права доступа к ним.

3.5.2 неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации (несанкционированное изменение, копирование защищаемой информации);

3.5.3 ошибки обслуживающего персонала при эксплуатации информационных систем;

3.5.4 несанкционированный доступ к защищаемой информации лицами, не имеющими права доступа к ней, а именно:

3.5.4.1 подключение технических средств к информационным системам;

3.5.4.2 использование закладочных устройств, маскировка под зарегистрированного пользователя;

3.5.4.3 использование недекларированных возможностей программного обеспечения;

3.5.4.4 использование программных закладок и применение программных вирусов;

3.5.4.5 хищение носителей защищаемой информации;

3.5.4.6 нарушение функционирования технических средств обработки защищаемой информации.

3.5.5 дефекты, сбои, отказы, программного обеспечения и аварии технических средств и систем обеспечения их отказоустойчивого функционирования;

3.5.6 природные явления, стихийные бедствия (пожары, наводнения, землетрясения, грозовые разряды).

4. Порядок управления инцидентами информационной безопасности

4.1. Общий порядок управления инцидентами информационной безопасности включает:

4.1.1 обнаружение и информирование об инциденте информационной безопасности;

4.1.2 регистрация инцидента информационной безопасности;

4.1.3 локализация и устранение последствий инцидента информационной безопасности;

4.1.4 расследование инцидента информационной безопасности и реализация действий, предупреждающих его повторное возникновение (корректирующие меры).

5. Обнаружение и информирование об инциденте информационной безопасности

5.1. При обнаружении инцидента информационной безопасности (или события безопасности информации, имеющего признаки инцидента) должен быть незамедлительно проинформирован Администратор информационной

безопасности (средствами служебной электронной почты и (или) посредством телефонной связи).

5.2. В случае невозможности информирования Администратора информационной безопасности об инциденте информационной безопасности (посредством телефонной связи) о случившемся инциденте информационной безопасности должен быть уведомлен (посредством телефонной связи) директор образовательной организации или лицо, его замещающее.

5.3. Сообщение о случившемся инциденте информационной безопасности должно содержать следующую информацию:

5.3.1 Ф.И.О., должность работника, выявившего инцидент информационной безопасности;

5.3.2 время обнаружения инцидента информационной безопасности;

5.3.3 описание инцидента информационной безопасности.

6. Регистрация инцидента информационной безопасности

6.1. Регистрация инцидентов информационной безопасности осуществляется Администратором информационной безопасности в журнале учета инцидентов информационной безопасности (форма журнала представлена в приложении 2 к настоящей Политике).

6.2. На каждый инцидент информационной безопасности Администратором информационной безопасности формируется карточка инцидента информационной безопасности (форма карточки приведена в приложении 3 к настоящей Политике).

6.3. До момента полного заполнения карточки инцидента информационной безопасности и, соответственно, закрытия инцидента она своевременно заполняется и ведется в электронном виде, после чего распечатывается и хранится на бумажном носителе.

6.4. На этапе регистрации инцидента подлежат заполнению следующие разделы карточки:

6.4.1 общие сведения об инциденте информационной безопасности;

6.4.2 содержание инцидента информационной безопасности;

6.4.3 воздействие инцидента на информационные ресурсы (системы) или средства обработки информации.

6.5. Критичность инцидента зависит от критичности информационных ресурсов (систем) или средств обработки информации, затронутых инцидентом, а также области распространения (действия) инцидента, и определяется по таблице 1:

Таблица 1 – Определение критичности информационного ресурса (системы) или средства обработки информации

Область распространения и действия инцидента ИБ	Критичность информационного ресурса (системы) или средства обработки информации		
	высокая	**средняя**	**низкая**
1	2	3	4
Выходящий за пределы образовательной организации	Высокая	Высокая	Средняя
Пределы отдельного структурного подразделения	Высокая	Средняя	Низкая
Пределы одной информационного ресурса (системы)	Средняя	Низкая	Низкая

7. Локализация и устранение последствий инцидента информационной безопасности

7.1. Срок реагирования на инцидент информационной безопасности напрямую зависит от степени критичности инцидента и составляет:

7.1.1 для инцидентов, имеющих высокую критичность, – незамедлительное реагирование;

7.1.2 для инцидентов, имеющих среднюю критичность, – срок реагирования не более одного рабочего дня;

7.1.3 для инцидентов, имеющих низкую критичность, – срок реагирования не более пяти рабочих дней.

7.2. Под реагированием на инцидент информационной безопасности понимается назначение ответственных лиц за локализацию и устранение последствий инцидента информационной безопасности. Ответственные лица назначаются Администратором информационной безопасности по согласованию с директором образовательной организации, или лицом, его замещающим.

7.3. В первую очередь осуществляется локализация инцидента информационной безопасности – предпринимаются все необходимые и доступные меры по сдерживанию/пресечению распространения негативного воздействия инцидента на информационные системы, а позже (или одновременно) проводятся работы по устранению последствий инцидента информационной безопасности. Могут назначаться различные ответственные за данные процессы лица.

7.4. Ответственные лица сообщают планируемый срок локализации и устранения последствий инцидента информационной безопасности, а также отчитываются Администратору информационной безопасности о степени выполнения работ.

7.5. Процесс локализации и устранения последствий инцидента информационной безопасности своевременно отражается в Карточке инцидента информационной безопасности.

8. Расследование инцидента информационной безопасности и реализация корректирующих мер

8.1. Процедура расследования инцидента информационной безопасности предназначена для выявления причин (условий и факторов), вызвавших инцидент информационной безопасности, и/или негативную тенденцию развития связанной с этим инцидентом ситуации, а также анализа и оценки адекватности и эффективности действий, предпринятых, по управлению инцидентом информационной безопасности.

8.2. Для проведения процедуры расследования инцидента информационной безопасности привлекается комиссия по обеспечению информационной безопасности (далее – комиссия по ОИБ), утвержденная приказом директора образовательной организации.

8.3. В процессе расследования инцидента информационной безопасности на основании анализируемых данных должен быть установлен нарушитель информационной безопасности (для внутренних категорий нарушителей – должно быть выявлено конкретное физическое лицо), чьи действия (умышленные или неумышленные) привели к возникновению инцидента информационной безопасности.

8.4. По итогам расследования инцидента информационной безопасности комиссией по ОИБ разрабатывается комплекс мер, направленных на:

8.4.1 недопущение (минимизацию вероятности) возможности повторения инцидента в будущем – разработка корректирующих мер;

8.4.2 выявление нарушителей информационной безопасности (если его не удалось установить в процессе расследования инцидента).

8.5. При разработке корректирующих мер должны учитываться их возможные воздействия на процесс функционирования информационных систем (в том числе должна быть оценена возможная степень негативного влияния на работу пользователей информационных систем), а также стоимость (экономическая обоснованность) реализации данных мер.

8.6. Результат разработки корректирующих мер (отчет) передается директору образовательной организации или лицу, его замещающему, для принятия дальнейших решений по реализации данных мер.

8.7. Процесс расследования инцидента информационной безопасности и реализация корректирующих мер своевременно отражается в Карточке инцидента информационной безопасности.

8.8. После выполнения всех действий по регистрации, локализации, устранению последствий, расследования инцидента информационной безопасности и принятия корректирующих мер инцидент должен быть закрыт (разрешен), о чем делается запись в журнале учета инцидентов информационной безопасности и карточке инцидента информационной безопасности.

9. Ответственность за исполнение положений настоящей Политики

9.1. Все работники образовательной организации обязаны информировать администратора информационной безопасности об инцидентах информационной безопасности, событиях безопасности информации (имеющих

признаки инцидента) и, при необходимости, принимать участие в расследовании инцидента информационной безопасности вместе с комиссией по ОИБ.

9.2. Администратор информационной безопасности несет ответственность за:

9.2.1 пересмотр (не реже одного раза в год) Перечня событий безопасности информации информационных систем образовательной организации;

9.2.2 принятие решения по реализации корректирующих мер (в соответствии с предоставленными отчетами);

9.2.3 регистрацию инцидентов информационной безопасности в Журнале учета инцидентов информационной безопасности;

9.2.4 согласование перечня лиц, ответственных за локализацию и устранение последствий инцидентов информационной безопасности;

9.2.5 ведение карточек инцидентов информационной безопасности;

9.2.6 определение лиц, ответственных за локализацию и устранение последствий инцидентов информационной безопасности;

9.2.7 контроль сроков локализации и устранение последствий инцидентов информационной безопасности;

9.2.8 анализ проведенной работы по локализации и устранению ответственными лицами последствий инцидентов информационной безопасности;

9.2.9 участие в составе комиссии по ОИБ в рамках расследования инцидентов информационной безопасности.

9.2.10 обеспечение непрерывности регистрации, учета, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации в соответствии с требованиями настоящей Политики (в зоне своей ответственности);

9.2.11 реализацию комплекса мер по защите сведений о событиях безопасности информации от неправомерного доступа, уничтожения или модифицирования (в зоне своей ответственности);

9.2.12 своевременный мониторинг и анализ событий безопасности информации с целью выявления информационной безопасности (в зоне своей ответственности).

9.3. Администратор информационных систем несет ответственность за:

9.3.1 обеспечение непрерывности регистрации, учета, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации в соответствии с требованиями настоящей Политики (в зоне своей ответственности);

9.3.2 реализацию комплекса мер по защите сведений о событиях безопасности информации от неправомерного доступа, уничтожения или модифицирования (в зоне своей ответственности);

9.3.3 своевременный мониторинг и анализ событий безопасности информации с целью выявления информационной безопасности (в зоне своей ответственности);

9.3.4 участие в составе комиссии по ОИБ в рамках расследования инцидентов информационной безопасности (при необходимости, определяемой администратором информационной безопасности).

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

Приложение 1
к политике управления
событиями безопасности
информации

ПЕРЕЧЕНЬ
типов событий безопасности информации, подлежащих регистрации в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Физический доступ к информационным ресурсам (системам), средствам обработки информации и средствам обеспечения их отказоустойчивости:

1.1.1 физический доступ работников и иных лиц в защищаемые помещения, не имеющих доступ в данные помещения;

1.1.2 физический доступ третьих лиц в защищаемые помещения (проводящих работы по обслуживанию, ремонту, сопровождению и настройке серверного, активного сетевого и прочего оборудования, располагающегося в помещениях);

1.1.3 изменение (в том числе замена, добавление или изъятие) состава средств обработки информации);

1.1.4 замена и (или) модификация аппаратной конфигурации средств обработки информации;

1.1.5 осуществление действий со съемными носителями информации;

1.1.6 осуществление действий с дополнительными идентификаторами, используемыми для доступа к информационным ресурсам (системам);

1.1.7 вынос за пределы организации средств вычислительной техники;

1.1.8 передача средств вычислительной техники между структурными подразделениями образовательной организации;

1.1.9 передача средств вычислительной техники и их компонентов в сторонние организации.

2. Использование информационных ресурсов (систем) и средств обработки защищаемой информации:

2.1.1 предоставление аутентификационной и ключевой информации на доступ к информационным ресурсам (системам) и средствам обработки защищаемой информации (в том числе по использованию служебной электронной почты и сети Интернет);

2.1.2 изменение прав доступа к информационным ресурсам (системам) и средствам обработки защищаемой информации;

2.1.3 изменение и (или) компрометация аутентификационной или ключевой информации;

2.1.4 аутентификация и идентификация пользователей информационных ресурсов (систем) и средств обработки защищаемой информации (в том числе неуспешная);

2.1.5 удаленный доступ к информационным ресурсам (системам) и средствам обработки защищаемой информации (с указанием протокола доступа);

2.1.6 действия, совершаемые с защищаемой информацией;

2.1.7 завершение сеансов работы пользователей информационных ресурсов (систем) и средств обработки защищаемой информации;

2.1.8 вывод на печать защищаемой информации;

2.1.9 отключение/перезагрузка или приостановление работы средств обработки защищаемой информации;

2.1.10 изменение параметров настроек средств обработки защищаемой информации;

2.1.11 изменение состава и версий программного обеспечения (в том числе баз сигнатур средств антивирусной защиты информации и средств обнаружения вторжений);

2.1.12 сбои и отказы работоспособности информационных ресурсов (систем) и средств обработки защищаемой информации;

2.1.13 восстановление работоспособности информационных ресурсов (систем) и средств обработки защищаемой информации;

2.1.14 архивирование, резервирование и восстановление защищаемой информации;

2.1.15 выполнение операций, связанных с эксплуатацией и администрированием информационных ресурсов (систем) и средств обработки защищаемой информации).

Настоящий перечень подлежит обязательному ежегодному пересмотру.

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 2
к политике управления событиями
безопасности информации

ФОРМА ЖУРНАЛА УЧЕТА
инцидентов информационной безопасности

№ п/п	№ карточки инцидента ИБ	Дата и время возникновения инцидента ИБ	Дата и время регистрации инцидента ИБ	Ф.И.О. и должность работника, обнаружившего инцидент ИБ	Критичность инцидента ИБ	Затронутые информационные ресурсы (системы) и средств обработки информации	Ф.И.О. и должность лица, ответственного за устранение инцидента	Дата и время устранения инцидента ИБ
1	2	3	4	5	6	7	8	9
1								
2								

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 3
к политике управления
событиями безопасности

ФОРМА КАРТОЧКА
инцидента информационной безопасности № ____

№ п/п	Наименование характеристики инцидента ИБ:	Описание
1	**2**	**3**
1. Общие сведения об инциденте ИБ		
1.1	Номер записи согласно Журналу учета инцидентов ИБ	
1.2	Дата и время возникновения инцидента ИБ	
1.3	Дата и время регистрации инцидента ИБ	
1.4	Источник информации об инциденте ИБ	работник или техническое средство
1.5	Ф.И.О. и должность работника, обнаружившего инцидент ИБ	
1.6	Контактные данные работника, обнаружившего инцидент	
1.7	Наименование технического средства, при использовании которого обнаружен инцидент ИБ	
1.8	Описание инцидента ИБ	
2. Содержание инцидента ИБ		
2.1	Сведения о нарушении установленных организационно-распорядительными документами требований по обеспечению ИБ	«нет» «наименование документа, регламентирующего требование; № пункта документа»
2.2	Данные о нарушителе требований по обеспечению ИБ	«нет» «Ф. И.О., должность нарушителя»
2.3	Категория инцидента ИБ	«случайный» «преднамеренный»
2.4	Тип инцидента ИБ	«свершившийся» «попытка осуществления инцидента ИБ» «подозрение на инцидент ИБ»
3. Воздействие инцидента на информационные ресурсы (системы) и средства обработки защищаемой информации		

1	2	3
3.1	Типы объектов (ресурсов), затронутых инцидентом	«файлы/базы данных, содержащие защищаемую информацию» «автоматизированные рабочие места» «серверы информационных систем» «активное сетевое оборудование» «средства защиты информации» «носители информации (в том числе бумажные носители)» «системное/прикладное программное обеспечение» «линии и сети передачи данных» «помещения, здания, сооружения, инженерные сети и коммуникации»
3.2	Нарушенные свойства безопасности:	«конфиденциальность» «целостность» «доступность»
3.3	Область распространения и действия инцидента ИБ	«пределы одного информационного ресурса (системы)» «пределы отдельного структурного подразделения» «государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» в целом» «выходящий за пределы государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»
3.4	Критичность инцидента ИБ	«высокая» «средняя» «низкая»
4. Локализация и устранение последствий инцидента ИБ		
4.1	Информирование об инциденте ИБ	«дата и время информирования и кому сообщено»
4.2	Назначение ответственного лица за локализацию инцидента ИБ	«дата и время, Ф.И.О., должность ответственного лица»
4.3	Планируемый срок локализации инцидента ИБ	«планируемый срок, определенный ответственным лицом»
4.4	Сведения о локализации инцидента ИБ	«дата и время, описание предпринятых действий»
4.5	Назначение ответственного лица за устранение последствий инцидента ИБ	«дата и время, Ф.И.О., должность ответственных лиц»
4.6	Планируемый срок устранения последствий инцидента ИБ	«планируемый срок, определенный ответственным лицом»
4.7	Сведения об устранении последствий инцидента ИБ	«дата и время, описание предпринятых действий»
5. Расследование инцидента ИБ и реализация корректирующих мер		
5.1	Сведения о комиссии по	«комиссия по ОИБ, состав ее членов»

1	2	3
	расследованию инцидента ИБ	
5.2	Сведения о причинах возникновения инцидента ИБ	«описание»
5.3	Сведения о лицах, понесших ответственность за инцидент ИБ	«Ф.И.О., должность лица, вид ответственности»
5.4	Степень вероятности повторного возникновения инцидента ИБ	«нет» «минимальная» «средняя» «высокая»
5.5	Перечень корректирующих мер, направленных на предупреждение повторного возникновения инцидента	«описание»

Дата, время закрытия инцидента ИБ: _____

Ф.И.О., подпись администратора ИБ _____

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)